



RECORDS COMPUTERS AND THE RIGHTS OF CITIZENS

XX 11
85
108 13

LIBRARY
Department of Justice

TRAFFIC
* 1201 to 1201000000



Report of the Secretary's Advisory Committee
on Automated Personal Data Systems

U.S. Department of Health, Education & Welfare

July 1973

DHEW Publication NO. (OS)73-94



DEPARTMENT OF HEALTH, EDUCATION, AND WELFARE

OFFICE OF THE SECRETARY

WASHINGTON, D.C. 20201

SECRETARY'S ADVISORY COMMITTEE ON
AUTOMATED PERSONAL DATA SYSTEMS

June 25, 1973

Honorable Caspar W. Weinberger
Secretary of Health, Education,
and Welfare

Dear Mr. Secretary:

It is a privilege for me to submit this report to you on behalf of the Secretary's Advisory Committee on Automated Personal Data Systems. The Committee believes that the report makes a significant contribution toward understanding many of the problems arising from the application of computer technology to record keeping about people. Our recommendations provide the framework for general solutions and also specify actions to be taken both within HEW and by the Federal government as a whole.

We are grateful for the interest that you have expressed in our work. Both you and former Secretary Richardson deserve praise for responding to public concern about the issues posed by automation of personal-data record-keeping operations. We have greatly appreciated the opportunity to be of service to you and the Department, and, we hope, to all our fellow citizens.

Our undertaking has required the cooperation of many agencies and organizations and the assistance of many individuals. We wish to thank everyone at HEW who helped us. The contributions of individuals who served as our immediate staff are acknowledged in the Preface to the report. We wish to note particularly the remarkable diligence and devotion to our task of our Executive Director, David B. H. Martin, and Associate Executive Director, Carole Watts Parsons.

Sincerely,

Willis H. Ware

Chairman

Foreword

Computers linked together through high-speed telecommunications networks are destined to become the principal medium for making, storing, and using records about people. Innovations now being discussed throughout government and private industry recognize that the computer-based record keeping system, if properly used, can be a powerful management tool. Its capacity for timely retrieval and analysis of complex bodies of data can be of invaluable assistance to hard-pressed decision makers. Its ability to handle masses of individual transactions in minutes and hours rather than in weeks or months, as was formerly the case, makes possible programs of service to people that would have been unthinkable in the manual record-keeping era. Medicare, for example, would be impossible to administer without computers to take over many routine clerical functions. Computer-based public assistance payments systems are also helping States and counties to assure that welfare payments go to those who truly need and deserve them. This Administration's strategy calls for strengthening direct support of individuals—for putting cash directly in the hands of those who need it—and keeping accurate, up-to-date, easily retrieved records on individual beneficiaries helps achieve that goal.

Nonetheless, it is important to be aware, as we embrace this new technology, that the computer, like the automobile, the skyscraper, and the jet airplane, may have some consequences for American society that we would prefer not to have thrust upon us without

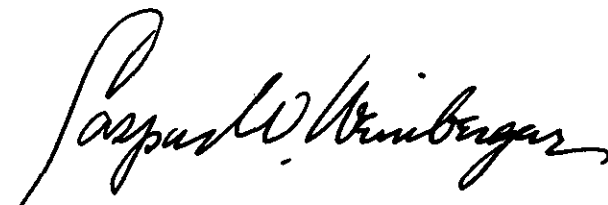
warning. Not the least of these is the danger that some record-keeping applications of computers will appear in retrospect to have been oversimplified solutions to complex problems, and that their victims will be some of our most disadvantaged citizens.

This report of the Secretary's Advisory Committee on Automated Personal Data Systems calls attention to issues of record-keeping practice in the computer age that may have profound significance for us all.

One of the most crucial challenges facing government in the years immediately ahead is to improve its capacity to administer tax dollars invested in human services. To that end, we are attempting to eliminate ineligibility, overpayment, and other errors from welfare caseloads. We are encouraging local government and public and private service agencies to forge new cooperative links with one another. We are attempting to move away from the fragmented social service structures of the past, which have dealt with individuals and with families as if their problems could be neatly compartmentalized; that is, as if they were not people. Many of these measures could result in more intensive and more centralized record keeping on individuals than has been customary in our society. Potentially, at least, this is a double-edged sword, as the Committee points out. On the one hand, it can help to assure that decisions about individual citizens are made on the basis of accurate, up-to-date information. On the other, it demands a hard look at the adequacy of our mechanisms for guaranteeing citizens all the protections of due process in relation to the records we maintain about them.

The report of the Secretary's Advisory Committee on Automated Personal Data Systems deserves to be widely read and discussed. It represents the views of an unusual mixture of experts and laymen. The Committee obviously considers its recommendations to be a reasonable response to a difficult set of problems. The Committee has taken a firm position with which some may disagree. However,

we should be grateful to the Committee for speaking with such a clear voice. In doing so, it has no doubt set in motion the kind of constructive dialogue on which a free society thrives.



July, 1973

Preface

This is a report about changes in American society which may result from using computers to keep records about people. Its central concern is the relationship between individuals and record-keeping organizations. It identifies key issues and makes specific recommendations for action.

The Secretary's Advisory Committee on Automated Personal Data Systems was established by former Secretary of Health, Education, and Welfare Elliot L. Richardson in response to growing concern about the harmful consequences that may result from uncontrolled application of computer and telecommunications technology to the collection, storage, and use of data about individual citizens. The formation of the Committee rests upon a public interest determination made by Secretary Richardson which provides in part as follows:

The use of automated data systems containing information about individuals is growing in both the public and private sectors. . . . The Department itself uses many such systems, and in addition, a substantial number. . . are used by other organizations, both public and private, with financial or other support. . . from the Department. . . . At the same time, there is a growing concern that automated personal data systems present a serious potential for harmful consequences, including infringement of basic liberties. This has led to the belief that special safeguards should be developed to protect against potentially harmful consequences for privacy and due process.

The Committee was asked to analyze and make recommendations about:

- Harmful consequences that may result from using automated personal data systems;
- Safeguards that might protect against potentially harmful consequences;
- Measures that might afford redress for any harmful consequences;
- Policy and practice relating to the issuance and use of Social Security numbers.

The Committee's membership encompassed a broad range of expertise and experience and an equally diverse range of viewpoints. Some members came from the social service professions where large-scale data banks are a fact of life, not a probable future development. Others came from management backgrounds in both government and private industry. Many have had practical experience in operating or using automated personal data systems in settings ranging from a nationwide credit-bureau network to the program management information system of a State government. Others came from the academy, and from parts of the research community concerned with applying knowledge developed by the information sciences. Two members of the Committee were State legislators; one was a labor union official; others were lawyers and private citizens.

Given this diversity, it should be no surprise that at our first meetings, in the spring of 1972, the views of individual members on the significance of applying computer technology to personal-data record keeping sometimes differed sharply. Many, indeed probably most, did not initially feel a sense of urgency about the potential ill effects of current practices in the design and operation of automated personal data systems. Some agreed that computer-based record keeping poses a latent danger to individual citizens, but looked optimistically to technological innovations, particularly access-control devices, to prevent problems from arising. Others painted dramatic portraits of the potential benefits of large-scale data networks to citizens in a densely populated, highly mobile

society—benefits that would accrue to all social and economic classes, enhancing knowledge, increasing the efficiency of social services, and expanding personal freedom.

Slowly, however, the attitudes of the members changed. Shared concerns took root as we heard testimony from over 100 witnesses representing more than 50 different organizations, and as we reviewed a substantial collection of written materials, including reports by similar commissions in this country, Canada, Great Britain, and Sweden. The Committee also gathered information on related studies and fact-finding efforts through a special inquiry to approximately 250 trade and professional associations and public interest groups. (Appendix A lists the individuals who appeared before the Committee and the groups and organizations to which our letter of inquiry was sent.)

Out of this array of personal contacts, written communications, and published documents, our report to the Secretary has emerged. We perceive ourselves as sharing concerns and perspectives expressed in other recent reports on computer-based record keeping, among them *Privacy and Computers* (1972), the report of a task force established jointly by the Canadian Departments of Communications and Justice; *Data and Privacy* (1972), the report of the Swedish Committee on Automated Personal Systems; and *Databanks in a Free Society* (1972), the report of the National Academy of Sciences Project on Computer Databanks.

Our undertaking has required the cooperation of many agencies and organizations and the assistance of many individuals to all of whom we are grateful. We thank all those in HEW who helped us, noting particularly the generous cooperation of Al Guolo, James J. Trainor, Mrs. Lottie C. Owen, and James D. Smith. The Assistance of those who worked as our immediate staff and consultants deserves special acknowledgement as follows:

For general research support and helping to make our meetings productive—Paul J. Corkery, John P. Fanning, Courtney B. Justice, Nancy J. Kleeman, Terrence D.C. Kuch, Carolyn Lewis, William L. Marcus, John J. Salasin, Leonard Sherp, Frederick H. Sontag, Lindsay Spooner, Jeffrey L. Steele, and Lynn Zusman;

For legal research and drafting—John P. Fanning;

For helping to prepare and edit drafts of the report and for preparing appendices — John P. Fanning, Terrence D.C. Kuch, Daniel H. Lufkin, Lindsay Spooner, and Patricia Tucker;

For typewriting and proofreading draft after draft of the report — Claire I. Hunkin, Rose Schiano, and Patricia Young;

For painstaking administrative support — Beverlyann Garfield, Ronald C. Lett, James F. Sasser, Rose Schiano, and Helen C. Szpakowski.

Finally, we wish to note especially the dedication and complete personal commitment to all aspects of the Committee's undertaking by David B.H. Martin, Special Assistant to the Secretary, who served as Executive Director for the Committee, and Carole Watts Parsons, Associate Executive Director. Without their patient prodding and tireless efforts, this report could not have been completed.

Willis H. Ware, *Chairman*
Secretary's Advisory Committee on
Automated Personal Data Systems

**SECRETARY'S ADVISORY COMMITTEE
ON AUTOMATED PERSONAL DATA SYSTEMS***

WILLIS H. WARE, Corporate Research Staff, The Rand Corporation, Santa Monica, California, *Chairman*

LAYMAN E. ALLEN, Professor of Law, University of Michigan Law School, Ann Arbor, Michigan

JUAN A. ANGLERO, Assistant Secretary for Planning & Development, Department of Social Services, Commonwealth of Puerto Rico

STANLEY J. ARONOFF, Ohio State Senator, Cincinnati, Ohio

WILLIAM T. BAGLEY, California State Assemblyman, Sacramento, California

PHILIP M. BURGESS, Professor of Political Science, The Ohio State University, Columbus, Ohio

GERTRUDE M. COX, Statistical Consultant, Raleigh, North Carolina

K. PATRICIA CROSS, Senior Research Psychologist, Educational Testing Service, Berkeley, California

GERALD L. DAVEY, President and Chief Executive Officer, Medlab Computer Services, Inc., Salt Lake City, Utah

J. TAYLOR DeWEESE, Philadelphia, Pennsylvania

GUY H. DOBBS, Vice President, Xerox Computer Services, Los Angeles, California

†**ROBERT R.J. GALLATI**, Director, New York State Identification and Intelligence System (NYSIIS), Albany, New York

FLORENCE R. GAYNOR, Executive Director, Martland Hospital, Newark, New Jersey

††**JOHN L. GENTILE**, Deputy Director, State of Illinois Department of Finance, Springfield, Illinois

***FRANCES GROMMERS, M.D.**, Visiting Lecturer, Harvard School of Public Health, Boston, Massachusetts

JANE L. HARDAWAY, Commissioner, State of Tennessee Department of Personnel, Nashville, Tennessee

JAMES C. IMPARA, Administrator of Educational Accountability, State of Florida Department of Education, Tallahassee, Florida

PATRICIA J. LANPHERE, Assistant Supervisor, Bureau of Services to Families and Children, State of Oklahoma Department of Institutions, Social and Rehabilitative Services, Oklahoma City, Oklahoma

ARTHUR R. MILLER, Professor of Law, Harvard Law School, Cambridge, Massachusetts

DON M. MUCHMORE, Senior Vice President, California Federal Savings and Loan Association, Los Angeles, California

JANE V. NOREEN, St. Paul, Minnesota

ROY SIEMILLER, Vice President, Labor Relations, National Alliance of Businessmen, Washington, D.C.

MRS. HAROLD SILVER, Denver, Colorado

SHEILA M. SMYTHE, Vice President, Associated Hospital Service of New York, New York, New York

JOSEPH WEIZENBAUM, Professor of Computer Science, Massachusetts Institute of Technology, Cambridge, Massachusetts

DAVID B.H. MARTIN, Special Assistant to the Secretary of Health, Education, and Welfare, *Executive Director*

CAROLE W. PARSONS, *Associate Executive Director*

*Biographical information on the members of the Committee will be found on pp. 333-337 below.

†On April 1, 1973, Dr. Gallati assumed responsibility as Commanding Officer, Inspection Division, Police Department, City of New York.

††On April 1, 1973, Mr. Gentile joined the U.S. Postal Service as Assistant Postmaster General, Management Information Systems Department.

*Dr. Grommers served as Chairman of the Committee from May, 1972 to January, 1973; she was unable to continue as a member of the Committee thereafter.

Contents

FOREWORD	v
PREFACE	viii
COMMITTEE MEMBERS	xii
SUMMARY AND RECOMMENDATIONS	xix
I. RECORDS AND RECORD KEEPERS	1
Historical Development, 1	
Types of Records About People, 5	
From Record Keeping to Data Processing, 7	
Systematic Management, 9	
II. LATENT EFFECTS OF COMPUTER-BASED RECORD KEEPING	12
Too Much Data, 13	
Easy Access, 15	
Technicians as Record Keepers, 22	
The Net Effect on People, 28	
III. SAFEGUARDS FOR PRIVACY	33
Personal Privacy, Record Keeping, and the Law, 33	
A Redefinition of the Concept of Privacy, 38	
Mechanisms for Providing Safeguards, 42	
The Costs of Safeguards, 44	

IV. RECOMMENDED SAFEGUARDS FOR ADMINISTRATIVE PERSONAL DATA SYSTEMS	48
Establishing Automated Personal Data Systems, 51	
The Safeguard Requirements, 52	
<i>Safeguard Requirements for Administrative Personal Data Systems</i> , 53	
Relationship of Existing Laws to the Safeguard Requirements, 64	
A Note on Mailing Lists, 71	
A Note on Intelligence Records, 74	
V. STATISTICAL-REPORTING AND RESEARCH USES OF ADMINISTRATIVE DATA SYSTEMS	78
Dimensions of the Problem, 78	
Mandatory or Voluntary Data Collection?, 80	
Assuring Sound Secondary Uses of Administrative Data Systems, 82	
Recommendations, 85	
VI. SPECIAL PROBLEMS OF STATISTICAL-REPORTING AND RESEARCH SYSTEMS	89
Background Observations, 90	
The Need to Protect Data Subjects from Injury, 92	
The Need for Freer Access to Data in Government Files, 94	
Recommendations for Statistical-Reporting and Research Systems, 95	
<i>Safeguard Requirements for Statistical-Reporting and Research Systems</i> , 97	
Statutory Protection Against Compulsory Disclosure 102	
VII. THE SOCIAL SECURITY NUMBER AS A STANDARD UNIVERSAL IDENTIFIER	108
Criteria for a Standard Universal Identifier, 109	
Implications of a Standard Universal Identifier, 111	
The Social Security Number (SSN) as an SUI, 112	
History of the Social Security Number and Its Uses, 114	

VIII. RECOMMENDATIONS REGARDING USE OF THE SOCIAL SECURITY NUMBER	124
Specific Recommendations on the Social Security Number, 125	
Right of an Individual to Refuse to Disclose the Social Security Number, 125	
Issuance of Social Security Numbers, 126	
Constraints on Use and Dissemination of Social Security Numbers, 130	
Prohibition of Non-Data-Processing Uses of the Social Security Number, 134	
IX. ACTION AGENDA FOR THE SECRETARY OF HEALTH, EDUCATION, AND WELFARE	136
Legislation, 136	
Administrative Action, 138	
Additional Action, 140	
Organizational Responsibility, 142	
Immediate Action, 142	
APPENDICES	
A. Meetings and Activities of the Secretary's Advisory Committee on Automated Personal Data Systems, 147	
B. "Computers and Privacy": The Reaction in Other Countries, 167	
C. Confidentiality and the Census, 1790-1929, 178	
D. The National Driver Register, 202	
E. Computerized Criminal Information and Intelligence Systems, 222	
F. Correctionetics: A Blueprint for 1984, 247	
G. The Law Relating to HEW Personal-Data 258	
H. Mailing Lists 288	
I. Bibliography on Record Keeping and Personal Privacy, 298	
Biographical Notes on Members of the Secretary's Advisory Committee on Automated Personal Data Systems, 333	

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.

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.

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 recommend that all Federal agencies (i) apply these safeguard requirements, by administrative action, to all Federal statistical-reporting and research systems, and (ii) assure, through formal rule making, that the safeguard requirements are applied to all systems within reach of the Federal government's authority. 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:

- (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

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, uses 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.

"The horror of that moment," the King went on, "I shall never, never forget!"

"You will, though," the Queen said, "if you don't make a memorandum of it."

Lewis Carroll
Through the Looking-glass

I

Records and Record Keepers

Historical Development

In Cabinet No. 1 of the Musée des Antiquités Nationales near Paris there lies a wing-bone of an eagle, not much longer than a finger. On it, three rows of tiny marks, each carefully engraved with a flint point, count off a calendar of days from new moon to new moon. That eagle bone from the Magdalenian period, roughly 14,000 years ago, is the most ancient evidence we have of man's unique ability use abstract notation as an aid to memory.

Out of the Stone Age, through the dawn of agriculture, similar records in all pre-literate cultures attest to the attempts of hunters, gatherers, and farmers to keep track of the passing of the seasons and the meshing cycles of growth and harvest on which survival depended. Even long after more complex societies had fostered more elaborate forms of written record keeping, simple tally scratches, half practical and half magical, continued to serve as records—on the tally sticks of millers, for example, and on the six-guns of lawmen.

Record-keeping techniques grew and were perfected as once-scattered tribes and small communities were amalgamated into larger and more organized states. Among the ancient cradles of civilization—Asia Minor, China, India, and Central and South America—only the Inca civilization of the Andes did not develop a written method of recording, using instead a system of knotted

cords, called *quipu*. Indeed, practically all the earliest writing deals with records—palace inventories, lists of tribute to kings and sacrifices to temples, records of royal births and deaths, traders' accounts—records of things too important to trust to memory.

In most of the ancient world, the scribes and clerks who developed systematic record keeping quickly expanded into generalized public administration. In Sumer and other city-states of Mesopotamia, royal genealogies were embellished with accounts of battles, land surveys included detailed descriptions of farms and villages, and tax records included commentaries on the tax laws that governed them. Gradually these commentaries were detached from records proper and took on a separate existence. The law code of Hammurabi, for example, emerged from the notes of scribes and marks an important milestone in the history of social organization. Once the laws of the state achieved an existence independent of records, the witness of the records could be used to bind the state and the citizen equally. When both the tax laws and the size of a man's herd were matters of public record, the pressure of public scrutiny would tend to keep both the publican and the herdsman honest.

Systematic record keeping in the ancient world reached a high point during the Roman Empire and then degenerated with the decline of strong central government. During the Middle Ages the levying of taxes was left largely in the hands of local strongmen who had little interest in record keeping. Although the laws of inheritance and the interest of the Church in proper sacramental procedures encouraged parishes to maintain registers of births, marriages, and deaths, those records seldom covered the bulk of the population. In some cases, however, rulers of newly conquered domains did order inventories and land surveys. One such was William the Conqueror's survey, known as the Domesday Book, of the extent and value of landholdings in England in A.D. 1086. It became the foundation of Exchequer records that, in turn, grew to include audits of the accounts of sheriffs and other local officials. The memory-aiding function of these records is suggested by the title of the official responsible for keeping them—King's Remembrancer.

As a landmark in the gradual evolution from personal sovereignty to bureaucratic administration, the Magna Carta of A.D. 1215 laid

the foundation in Anglo-Saxon legal tradition for codifying mutual responsibilities of government and governed. The Magna Carta, wrested from King John by his powerful barons, reduced the independence of justices, sheriffs, and other local officials, ensuring, in theory at least, that men who knew the common law and were willing to observe it would hold positions of high authority. During the reign of King John also, an administrative distinction between public and closed records began to be observed; official records were divided into *letters patent* that were sent and stored open, with the king's seal attached for authentication, and *letters close* that were sent folded and sealed, and that were stored secure from public inspection. The use and content of these two classes of records corresponds well, as we shall see, with the modern practice of separating public from confidential records.

As custom and statute more and more provided that government records should be open to the public, the justification for closed or secret records came to be their pertinence to the defense and security of the state. By the mid-1600's, all royal courts maintained files¹ of information on the identity and activities of citizens or aliens who were considered a threat to the state or the sovereign. Such files covered a small number of individuals by today's standards, but were treated with great secrecy and came to be the responsibility of a special class of record keeper well outside the regular channels of administration. The scope and intensity of this special field of record keeping soon gave it a character so different from its bureaucratic origins that it becomes convenient at this point to draw a distinction between general *administrative* records and the very special *intelligence* records.

As the idea gradually spread that governing a state involved more than determining and following the wishes of a small ruling class, government became less desultory, more aligned to philosophical currents, and less reactive to the press of random events. As government thus grew more self-conscious, the need for planning became apparent. At first, legislators used their right of access to public records mainly to look backwards; to reconstruct the flow of

¹ The use of the word "file" in this sense dates from the 1640's. See "File," *Oxford English Dictionary*, 1933, IV, 210.

history that had brought them to their present position. However, lawmakers bent on reform soon found that they needed better guides than records of legal decisions, royal correspondence, and official accounts and audits. They needed benchmark information from which to measure progress toward the goals they wish to achieve.

About 1750, the notion of a national census was revived for the first time since the Roman era. Public opposition was strong at first, many people suspecting a scheme to raise taxes. The clergy, for whom the Biblical injunction against the taking of a census still held,² also were opposed. Resistance gradually subsided; first in Scandinavia and the German states, then generally throughout the Continent and North America. In the American democracy, where a State's Congressional representation constitutionally depends in part on the size of its population, a national census, at least to the extent of a simple head count, was an obvious political necessity.

Government soon found that although there was little organized public objection to the head count as such, probing by census takers for information about income, family life, living habits, and other personal matters turned citizens obstinate and made the census more difficult to take.

The problem of gathering information from an antagonistic public led to the creation of yet another class of official records, the so-called *statistical*³ file. The essence of such a file is that the data it contains are not used to affect specific individuals. In creating such a file, the government, in order to gain information the public might otherwise be reluctant to give, foregoes some of the power over individuals that administrative records containing the same data would afford. The essential condition is that citizens believe that their individual contributions to a statistical file will not be made public and will not be used to punish or embarrass them.

² II Samuel 24 and I Chronicles, 21, 23, 27.

³ The word *statistics* [state-istics] came into use in the late 18th century to denote information on the condition of a state. See "Statistics," *Oxford English Dictionary*, 1933, X, 864.

Types of Records About People

As we approach the computer age in this brief survey of record keeping, we need to define the three main types of records that have been distinguished historically.⁴

Administrative Records. The administrative record is often generated in the process of a transaction—marriage, graduation, obtaining a license or permit, buying on credit, or investing money. Usually a record that refers to an individual includes an address or other data sufficient for identification. Personal data in an administrative record tends to be self-reported or gathered through open inspection of the subject's affairs. Private firms usually treat administrative records pertaining to individuals as proprietary information, while administrative records held by the government are normally accessible to the public and may be shared for administrative purposes among various agencies. Administrative records sometimes serve as credentials for an individual; birth certificates, naturalization papers, bank records, and diplomas all serve to define a person's status.

Intelligence Records. The intelligence record may take a variety of forms. Familiar examples are the security clearance file, the police investigative file, and the consumer credit report. Some of the information in an intelligence record may be drawn from administrative records, but much of it is the testimony of informants and the observations of investigators. Intelligence records tend to circulate among intelligence-gathering organizations and to be shared selectively with organizations that make administrative determinations about individuals. Intelligence records are seldom deliberately made public, except as evidence in legal proceedings.

⁴ The classification follows that of Prof. Alan Westin in M. Greenberger (Ed.), *Computers, Communications, and the Public Interest* (Baltimore, Md.: The Johns Hopkins Press), 1971, p. 156.

Statistical Records. A statistical record is typically created in a population census or sample survey. The data in it are usually gathered through a questionnaire, or by some other method designed to assure the comparability of individual responses. In nearly all cases, the identity of the record subject is eventually separated from the data in the record. If a survey must follow a given individual for a long time, his identity is often encoded, with the key to the code entrusted to a separate record to guard anonymity. Data from administrative records are sometimes used for statistical purposes, but statistical records about identifiable individuals are generally not used for administrative or intelligence purposes.

Not every record falls clearly into one of these three categories. The contemporary personnel record combines features of both administrative and intelligence records, and the records in the modern "management information system" have both administrative and statistical uses. Many records share characteristics of all three types to some degree. Yet whether one looks at the relationships among records of different types historically, from the perspective of present-day public policy, or from the point of view of the individuals who are the subjects of records, it is apparent that, by and large, administrative records are considered public; intelligence records, secret; and statistical records, anonymous. Moreover, democratic traditions with respect to the maintenance of *government* records about people have deep historical roots in a number of countries,⁵ and appear to be dominated by three major principles.

- An organization should record only information that has a clear-cut relevance to its concerns. Religious data, for example, should not be recorded where there is no state supported church, and citizens should not be required to furnish extraneous data as the price of obtaining a benefit.

⁵The reader who is interested in comparing the American experience with that of other nations will find a summary of available material in Appendix B, below.

- As much as possible, information that has been collected should be held in public files so that public scrutiny can act as a check on the arbitrary exercise of administrative authority. Closed files in government should be the exception, and their content and use should be regulated by specific laws, both to limit their extent and to assure their confidentiality.⁶
- The three types of records described above should be held separately, and each should be used only for its nominal purpose. The transfer of data from one type of record to another should take place only under controlled conditions. Records that do not fall neatly into one category, and record systems whose structure or use blurs the boundaries between types of records, demand special safeguards to protect personal privacy.

From Record Keeping to Data Processing

In this country, the end of World War II unleashed the deferred wants and pent-up purchasing power of the war years onto a labor-poor, capital-rich market. To help deal with the social and economic dislocations created, first, by demobilization, and later, by the Cold War, government kept in force many of the controls it had established during the years of all-out mobilization. The nation's pride in its wartime accomplishments lent a tone of confidence to even the most ambitious planning. Industry, for its part, took advantage of new technologies emerging from wartime research and development to make revolutionary changes in its methods of producing and distributing goods and services.

Acting together, these forces rapidly expanded commercial and governmental activities in the late forties and early fifties, forcing a vast increase in the volume of transactions requiring records about people. Compared with pre-war years, the number of bank checks written, the number of college students, and the number of pieces of mail all nearly doubled; the number of income-tax returns

⁶The evolution of Federal policy with respect to the confidentiality of census data is traced in Appendix C, below. See also Daniel J. Boorstin, *The Americans: The Democratic Experience* (New York: Random House), 1973, Chapters 19-28.

quadrupled; and the number of Social Security payments increased by a factor of more than 35.⁷

Technology developed during the war years was available to meet the challenge posed by this rising tide of recorded transactions. Automated data processing, transplanted from its military origin, quickly blossomed into a powerful industry, feeding on the demands of commerce and government for fast and efficient data handling, and in turn, fueling that demand by significantly changing the philosophy and practice of management itself. Since most industries based on a highly technical product must quickly develop a mass market to recover the high development and tooling costs, the computer industry devoted much attention and talent to marketing its products, without appreciating the implications of the technological revolution it was unleashing.

By the 1960's, attractive prices, persuasive salesmen, and ingenious computer software services had stimulated the introduction of automated data processing equipment into a great many record-keeping organizations, sometimes with far too little attention to the objectives and costs of automation. Although there were many examples of diseconomies and a few outright failures, the successes were so spectacular that the prestige of having a large-scale data processing capacity often prompted managers to keep their computers running, even at a financial loss.

The computer scored its earliest successes as a record keeper in fields where the data were mainly numerical. The speed with which the computer can do complex arithmetic, and the compactness of numerical data as compared to natural language, were major factors in quickly amortizing the considerable expense of installing a computer, and of converting an established record-keeping operation to take full advantage of the computer's capabilities. Thus, the earliest successes were heavily concentrated in science and engineering, banking, insurance, and accounting, and, above all, in the space program, where the value of computers in handling the intricate logistics of production, assembly, and testing was soon discovered.

⁷ Alan F. Westin, and Michael A. Baker, *Databanks in a Free Society* (New York: Quadrangle Books), 1972, pp. 224-225.

Systematic Management

For computers to be used effectively as management tools, an organization must first analyze its activities in a careful, systematic way. For example, if it is known that the goals of an operation can be attained by more than one method, the various alternatives can in principle be simulated on the computer, and their relative costs and benefits thereby compared to find the most cost-effective one. This mathematical simulation of a complex activity is called *systems analysis*.

During the late sixties, planners began to extend the techniques of systems analysis from their early engineering applications to more general problems of society. In particular, systems analysis was brought to bear on such ambitious tasks as improving the delivery of health care, managing the rapidly growing welfare caseload in urban centers, and measuring the effectiveness of a fragmented and increasingly expensive educational system.

The introduction of the disciplined methods of computer-assisted management gave program managers new tools for "auditing" the performance of institutions in programs of service to people. This auditing process includes:

- Keeping track of transactions between an organization and its clients or beneficiaries;
- Measuring the performance of the organization in relation to the goals set for it;
- Providing information needed for planning.

Each of these functions involves information about individuals. Administrative data are needed for everyday management of individual transactions. Statistical data are needed for planning and for assessing the performance of a program. Intelligence data are needed for making judgments about people's character and qualifications; e.g., in making suitability determinations for employment, commercial credit, welfare assistance, tuition-loan aid, or disaster relief.

The demand generated by all these uses for personal data, and for record-keeping systems to store and process them, challenges conventional legal and social controls on organizational record

keeping. Records about people are becoming both more ubiquitous and more important in everyday life. The number of organizations performing service and control functions is growing. In many cases, the scale of their operations virtually assures that the individuals they affect will be known to them only through the contents of systematically maintained records. A new technology is also demonstrating its potential to accommodate radical growth in organizational record-keeping operations. Yet society currently affords little protection for an individual who is the subject of a record, unless some commercial or property interest is involved.

The following chapters represent our effort to demonstrate why this situation deserves immediate attention and to recommend a course of action that, we believe, constitutes an appropriate societal response to the problems at hand.

The potency of these data does not lie in their voluminousness, even where the assembled information does provide something like a full sketch of the person concerned. Rather, the strength of the data stems from its ability to bear meaningfully, unambiguously and quickly on decision-making problems faced by the systems. Specifically, the files are most useful where they enable the system quickly and unerringly to single out the minority of their clients who warrant some measure of social control. In their most refined form, these discrimination procedures involve highly subtle judgements, often predictive ones about the client's future behaviour, based on imaginative and interpretive use of the discrete facts on file.

The press for economy in the compilation of data is matched in the patterns of its application to social control. Any of these systems can, for example, dispatch a representative expressly to accost delinquent clients; but as a regular measure this technique is difficult and expensive. Instead, the emerging pattern appears to be the extension of possible points of routine contact with the clientele, points through which clients must pass for their own purposes. At these points, the systems seek to develop means of quick identification and rapid information flow to enable them to bring the full weight of people's records to bear in decision-making about them—and, where necessary, in action against them. As the inducements to place oneself in touch with these points becomes more potent, the efficiency of these operations increases.

James B. Rule, *Private Lives and Public Surveillance*, 1973

II

Latent Effects of Computer-Based Record Keeping

The dangers latent in the spread of computer-based personal-data record keeping stem, in our view, from three effects of computers and computer-related technology on an organization's record-keeping practices.

- Computerization enables an organization to enlarge its data-processing capacity substantially.
- Computerization greatly facilitates access to personal data within a single organization, and across boundaries that separate organizational entities.
- Computerization creates a new class of record keepers whose functions are technical and whose contact with original suppliers and ultimate users of personal data are often remote.

These three effects on personal-data record-keeping are seldom observed in isolation from one another. Indeed, they are usually interdependent and may acquire a self-reinforcing momentum. The discussion that follows is focused on their potentially adverse consequences for individuals, for organizations, and for the society as a whole. It concentrates on aspects of computer-based record keeping

that highlight the influence of the technology, but also recognizes that organizational objectives, bureaucratic behavior, and public attitudes account in part for many of the potentially undesirable effects we have identified.

Too Much Data

The bare statement that computerization enables an organization to enlarge its capacity to process information deserves amplification. Although the computer *enables* a large organization to handle more data, the cost of changing from a manual to an automated operation may practically *compel* a smaller organization to exploit its data-processing capacity more fully. The cost of setting up an automated system includes not only that of equipment and special facilities, but also the cost of system analysis and design, of writing and testing computer programs, and of converting manual records into computer-accessible form. Thus, the manager of a newly automated system may have a strong economic incentive to spread the initial cost over as large a data-processing volume as he can, and to economize wherever possible in providing services that do not make a direct contribution to the efficient operation of the system itself. A typical result of this condition is that clients receive erroneous bills, unjustified dunning letters, duplicate magazine subscriptions, and countless other symptoms of inadequate system design and operation. Although these may be more a nuisance than a threat, they contribute heavily to the popular image of computerization as an offending and intrusive phenomenon.

The annoyance factor is worth more attention than many system managers give it. Resentment engendered in customers at the mercy of a computerized billing system, for example, spills over onto other computer operations, making unemotional discussion of computerization in fundamentally more significant contexts difficult.

An early incentive to concentrate on efficiency may also foster a tendency to behave as though data management were the primary goal of a computer-based record-keeping operation. When this occurs, unnecessary constraints may be placed on the gathering, processing, and output of data, with the result that the system becomes rigid and insensitive to the interests of data subjects. A

commonly observed tendency in these situations is to make the data subject do as much of the data collection work as possible by forcing him to decide how to fit himself into a highly structured, but limited set of data categories (e.g., "Please check one of the following boxes.").

This can be a way to cut down errors in transcribing data from one form of record to another, but when done solely in the interest of economy the system may well sacrifice flexibility and accuracy. It is true that data compression and "shorthand" record entries did not originate with the computer; ill-adapted categorization has been the bane of bureaucracy for generations. However, manual record keeping can, at the stroke of a pen, take account of data that do not fit comfortably into pre-conceived categories, while a computer record is not usually amenable to any sort of annotation that was not expressly planned for in the design of the system. The relative inflexibility of computer-based record keeping, coupled with the constraints that some automated systems put on the freedom of data subjects to provide explanatory details in responding to questions, contributes to the so-called "dehumanizing" image of computerization.

A recent occurrence in France illustrates how the inflexibility of an automated personal data system can adversely affect large numbers of people.¹ The computer facility of the national family allotment system, which disburses some \$600 million annually to 700,000 families in the Paris area, succumbed to the confusion created by changes in the allotment rate for nonworking wives, young people, and the handicapped. Efforts to unravel the difficulty were unsuccessful, and the computer center had to be reorganized as a manual operation in order to clear up an enormous backlog of emergency allotment payments. The disruption of human lives resulting from the inability to use the computer-based payments system was undoubtedly great and demonstrates why the difficulty of making even minor changes in the computer programs of a complex system gives cause for concern. Human bureaucracies exhibit similar rigidities, but their procedures can usually be changed by management directive, often by a simple promulgation of rules, and in a reasonably short time. In computer systems, how-

¹ *New York Times*, January 26, 1973, p. 4.

ever, even a change that has the wholehearted support of all concerned may be difficult and slow to effectuate.

This problem can become even more serious when economies of scale are sought by consolidating the data-processing tasks of several organizations into one automated system serving all. The effects of dysfunction then fall not only on the customers of the system primarily at fault, but also on "bystander" data subjects and other organizations.

Easy Access

The second effect of computerization on personal-data record keeping—that it facilitates access to data within a single organization and across boundaries normally separating organizations—is another source of concern. Quick, cheap access to the contents of a very large automated file often prompts an organization or group of organizations to indulge in what might be called "dragnet" behavior.²

An example of how a very carefully planned data system of ostensible social benefit operates as a dragnet is the National Driver Register of the Department of Transportation (more fully described in Appendix D). It provides a central data facility containing the names of individuals whose driver licenses are denied or withdrawn by a State. The purpose of the Register is to give each State access to the current revocation records of all other States, so that one may, if it wishes, avoid issuing a license to an individual whose license has been denied or withdrawn by another State.

Suppose that Missouri revokes John Doe's license for a serious offense. Doe applies in Illinois for a license, neglecting to mention the Missouri revocation. If Illinois issues Doe a license, it in effect nullifies Missouri's action, without knowing it is doing so. Before the National Driver Register was established, Illinois would have had to make specific inquiry to all other States in order to discover the Missouri record of license withdrawal. Because this was time-

² Although the term "dragnet" commonly connotes a system for catching criminals or others wanted by the authorities, the term, as used here, refers to any systematic screening of all members of a population in order to discover a few members with specified characteristics.

consuming, States tended to do it only for blatantly suspicious cases with the presumable result that many fraudulent applications were never detected. Now that Doe's record of license withdrawal goes into the master file of the National Driver Register, however, one query to the Register from Illinois will bring the Missouri action to light within 24 hours, thus permitting Illinois to make a decision to grant or withhold a license based upon the original Missouri record.

How can a system whose only purpose is to prevent fraud by drivers of demonstrated unfitness have any adverse effect? The answer lies in the efficiency of the Register; it has become easier for most States to put *all* their license applications routinely onto magnetic tape to be searched against the Register's file, rather than to separate out the suspicious cases for special treatment. If one accepts the objectives of the system—to identify irresponsible or incompetent drivers, and thus to reduce the number of traffic fatalities—this is not in itself an objectionable practice. However, automated matching of queries against NDR records generates identity matches so imprecise that subsequent manual screening reduces the system's 5000 possible "hits" per day to about 500 probable ones. Of the probable hits, the operators of the Register estimate that about three quarters are true identifications; that is, they definitely relate to an individual who has misrepresented himself in a license application. Arithmetic does the rest; a quarter of the probable hits—125 individuals per day—may find that they are required to prove that their licenses have not been withdrawn. In theory, a reply from the Register is supposed to be treated merely as a "flag" to inform the inquiring State that there may be a record on the individual about whom the query was made in the revocation files of another State. At least one State, however, makes the "flagged" applicant bear the full burden of proving that such a record does not exist. Here, the "dragnet effect" of cheap and easy data access—the fact that it is cheaper and more efficient to search the NDR on every license application—has resulted in occasional nuisance and potential injustice to some applicants.

The problems that can arise from the operation of the NDR stem from its role as a clearinghouse for information supplied and used by more than 50 independent driver licensing jurisdictions whose operations it does not control. Each jurisdiction using the Register

risks being misled by incomplete or erroneous data submitted by another participating jurisdiction. Although mistakes propagated by the NDR can usually be corrected at small expense in time and trouble, other multi-jurisdictional clearinghouses can have potentially more serious effects on individuals. The criminal history file of the FBI's National Crime Information Center (NCIC) is one example.

The NCIC is a computerized clearinghouse of information about wanted persons, stolen property, and criminal history records³ that will eventually provide criminal justice agencies throughout the United States with computer-to-computer access to the data in its files. The ultimate objective of the NCIC criminal history file is to enable law enforcement agencies, courts, and correctional institutions to determine, in seconds, whether an individual has a criminal record. The NCIC would appear to lack the potential to be used as a dragnet because inquiries are made only about particular individuals with whom law enforcement agencies have contact under conditions that constitute cause for suspicion of wrongdoing. In this respect, it differs significantly from the operation of the National Driver Register. Furthermore, the problem of mistaken identification in using the criminal history files should not arise because of NCIC's requirement that fingerprints be used to identify arrest and offender records entered into the system. (Errors of identification can and do occur in using the records in the wanted persons files because these are not identified by fingerprints. However, the ease with which inquiries can be made from remote terminals located in law enforcement and criminal justice agencies all over the country could lead to access to the NCIC criminal history files by more users and for checking on more individuals than is socially desirable.

Leaving aside the question of the probative value of arrest records, about which lively controversy exists, the consequences of excessive use of criminal history files might be innocuous if the NCIC records could be completely reliable. In practice, however, the NCIC, like the National Driver Register, does not have effective control over the accuracy of all the information in its files. The

³ See Appendix E for a discussion of the development of computerized criminal justice information systems in the United States.

NCIC is essentially an automated receiver, searcher, and distributor of data furnished by others. If a subscribing system enters a partially inaccurate record, or fails to submit additions or corrections to the NCIC files (e.g., the recovery of a stolen vehicle or the disposition of an arrest), there is not much that the NCIC can do about it.

Furthermore, the risk of propagating information that may lead to unjust treatment of an individual by law enforcement authorities in subscribing jurisdictions cannot be fully prevented.⁴

The NCIC checks on records being entered into its files, and periodically audits its files to try to assure that system standards for completeness and accuracy of records are being met. When it detects errors or points of incompleteness, it can seek corrective action and can flag its records to warn users of possible deficiencies. In the cases of an arrest record, however, even if the source agency does eventually submit information about the disposition of the arrest, there is no way that the NCIC can assure that all those who have had access to the record in the interim will receive the disposition information. Once a subscribing police department contributes an arrest report to the NCIC, that report is available to any qualified requestor in the system. In some States, this means that employers and licensing agencies (for physicians, barbers, plumbers, and the like) will have access to the record under State laws that require an arrest-record check on candidates for certain types of occupational certification. Thus, unless a criminal record information system is designed to keep track of all the ultimate users of each record released, and of every person who has seen it, any correction or emendation of the original record can never be certain to reach each holder of a copy.

Systems like the NCIC and the National Driver Register illustrate

⁴The NCIC system has been imitated by many city police departments whose systems respond to inquiries from law enforcement jurisdictions in adjacent suburbs. A suburban law enforcement officer first queries the city system to which his terminal is linked; if the file search there yields nothing, his query is passed on automatically to the State system and from there to the NCIC. These local systems have all the accuracy problems of the NCIC and some are currently the objects of law suits brought by their hapless victims. See, for example, "S.F.'s Forgetful Computer," *San Francisco Examiner*, May 9, 1973, p. 3, and "Coast Police Sued as Computer Errs," *New York Times*, May 5, 1973, p. 23. Almost all of these cases involve the failure of a local jurisdiction to report the recovery of a stolen vehicle or the revocation of a warrant.

one of the potentially most significant effects of computerization on personal-data record keeping—the enhanced ability to gather, package, and deliver information from one organization to another in circumstances where lines of authority and responsibility are overlapping or ambiguous, and where the significance attached to data disseminated by the system may vary among subscribing organizations. Unless all organizations in a multi-jurisdictional system can be counted on to interpret and use data in the same way, the likelihood of unfair or inappropriate decisions about the individual to whom any given record pertains will be a problem, and a particularly acute problem whenever records are incomplete or compressed. The records of school children, for instance, while highly comparable within a single school district, will be less so among the districts of a single State, and even more disparate among different States. Thus, data systems that are established deliberately to pass information across jurisdictional lines must be very carefully designed so as to foster sensitive, discriminating use of personal data.

The untoward effects of such systems (or of any system, for that matter) do not stem in the main from poor technical security. Although public mistrust of the computer often centers on the possibility of unauthorized access to a central data bank for purposes of blackmail or commercial exploitation (such as the clandestine copying of a list of names and addresses), the purely technical difficulties that can be placed in the path of any but the most well-equipped intruder can make almost every computer installation more secure than its manual counterpart. Unless an intruder has detailed technical knowledge of the system, and possibly also clandestine access to the facility itself, most systems can be quite well defended against "unauthorized" access (although at the present time many systems may not be well-defended). The problem is how to prevent "authorized" access for "unauthorized" purposes, since most leakage of data from personal data systems, both automated and manual, appears to result from improper actions of employees either bribed to obtain information, or supplying it to outsiders under a "buddy system" arrangement.

Concern about abuses of authorized access to "integrated" data systems maintained by State and local governments can have a particularly debilitating effect on people's confidence in their

governmental institutions. Ambitiously conceived integrated systems, no matter how secure technically, may have the effect of blurring, either in fact or appearance, established lines of political accountability and constitutionally prescribed boundaries between branches of government. When different branches arrange to share an integrated data-processing facility and its data, the executive usually will operate it. This happens partly because operational functions are normal for the executive, and partly because executive agencies usually have more experience with computer systems. It leads people to fear, however, that the needs of executive claimants may be met before the needs of legislative bodies and the judiciary. The priority system for allocating computer support will, of course, look fair on paper, but in practice the result may often be to shortchange the passengers on the system in favor of the driver.⁵ The recent development of mini-computers, much cheaper than the big systems of only five years ago but of comparable power, is providing an attractive economic alternative to large integrated systems. Large systems, however, are also becoming less expensive and there is no assurance that they will not become even more so as the result of new technological advance.

Finally, in terms of the historical classification of records in Chapter I, we recognize that combining bits and pieces of personal data from various records is one way of creating an intelligence record, or dossier. The possibility of using a large computer to assemble a number of data banks into a "master file" so that a dossier on nearly everybody could then be extracted is currently remote, since the ability to merge unrelated files efficiently depends heavily upon their having many features of technical structure in common, and also on having adequate information to match individual records with certainty.⁶ These technical obstacles are

⁵ For a discussion of political issues raised by computer-based information systems in urban government, see Anthony Downs, "The Political Payoffs in Urban Information Systems," in Alan F. Westin (Ed.), *Information Technology in a Democracy* (Cambridge, Mass.: Harvard University Press), 1971, pp. 311-321.

⁶ In addition to incompatibilities of file structure, the expectation that some day "it will all be put together" also runs afoul of the tenacity with which record-keeping

avoided if the capability to merge whole files is designed into a group of systems at the outset, a practice now characteristic of only a few multi-jurisdictional systems but perhaps becoming more prevalent. At the present time, however, compiling dossiers from a number of unrelated systems presents problems that few organizations, and probably no organizations outside of government, have the resources to solve.⁷

Nonetheless, public concern about such combinations of data through linkings and mergers of files is well founded since any compilation of records from other records can involve crossing functional as well as geographic and organizational boundaries. When data from an administrative record, for example, become part of an intelligence dossier, neither the data subject nor the new holder knows what purpose the data may some day serve. Moreover, the investigator may believe that no detail is too small to put into dossier, while the subject, for his part, can never know when some piece of trivia will close a noose of circumstantial evidence around him. Public sensitivity to the possibility of such

(Continued)

organizations tend to protect their own turf. Certainly among private organizations competitive pressures sometimes inhibit the free circulation of information about clients and also induce resistance to sharing large blocks of individually identifiable data with government agencies. The California Bankers Association, for example, is currently involved in litigation (*Stark v. Connally*, 347 Fed. Supp. 1242, 1972) to prevent the Treasury Department from enforcing the reporting provisions of the so-called Bank Secrecy Act of 1970 (12 U.S.C. 1829b; 31 U.S.C. 1051-1122) with respect to domestic financial transactions.

⁷ It should be noted that the same characteristics of automated systems which inhibit the compilation of dossiers can also inhibit efforts by the press and public interest groups to penetrate the decision-making processes of record-keeping organizations and expose them to public scrutiny. This is particularly true when organizations destroy "hard-copy" records after putting the information in them into computer-accessible form. In such cases, the computer can become a formidable gatekeeper, enabling a record-keeping organization to control access to public-record information that previously had been available to anyone with the time and energy to sift through its paper files. Putting public-record data in computer-accessible form can also increase the cost of piecing information together from several different files. The same programming costs that make it uneconomical for law enforcement investigators and private detectives to "fish" in the automated files of a credit bureau could also make it prohibitively expensive for private citizens to examine public records.

situations argues strongly for preserving the functional distinctions between different classes of personal data systems.

Technicians as Record Keepers

The reputation of the computer for impersonality and inhuman efficiency is due, in part, to the publicity given the computer as a poet, a chess-player, and a translator of exotic languages. "Machine intelligence" is a subject with fascinating technical and philosophical aspects. To date, however, there is no evidence that a computer capable of "taking over" anything it was not specifically programmed to take over is attainable. Indeed, as pointed out earlier, programming a computer to handle anything complicated is usually a very difficult and expensive job, requiring generous amounts of money, expertise, and management capability.

It seems safe to predict that economic and organizational constraints on the uses of computers will not change radically during the next few years. Although computing power and data-storage capability are steadily becoming cheaper, and problem-oriented programming is being improved, no dramatic breakthroughs are in sight. This prediction, however, cuts two ways. If we can comfortably assume that computers will not take control of anything on their own volition, we may still feel some disappointment that the application of computers will tend to remain in the hands of trained specialists whose competence is primarily in data processing rather than in the fields that data processing serves. Some would say that this circumstance results from an abdication by managers of their proper role, but whatever the reason, the effect can easily be to insulate the record-keeping functions of an organization from the pressures of both consumers and suppliers of data.

The presence of a specialized group of data-processing professionals in an organization can create a constituency within the organization whose interests are served by any increase in data use, without much regard for the intrinsic value of the increased use. The point is underlined by an experience common to many organizations. Some unit is already operating a computer facility for accounting, processing scientific or engineering data, or for some

other straightforward application to which the technology is well-adapted. Because the facility has extra computer time available, it is soon discovered that attractive software packages can be purchased to enable the computer to enlarge its scope and become a "management information system."

Such systems are founded on the proposition that efficient decision making requires that managers have available to them a greater or more timely supply of relevant information than they have been getting. As commonly observed, however, most managers do not need more of relevant information nearly as badly as they need less of irrelevant raw data.⁸ Thus, until the theory of management itself has progressed to a stage where the necessary data content of management-oriented systems can be predicted, their users are likely to find them disappointing.

Another, potentially more serious, consequence of putting record keeping in the hands of a new class of data-processing specialists is that questions of record-keeping practice which involve issues of social policy are sometimes treated as if they were nothing more than questions of efficient technique. The pressure for establishing a simple, identification scheme for locating records in computer-based systems is a case in point.

The technical argument for having a standard universal identifier for records about individuals focuses on increasing the efficiency of record keeping and record usage. Proponents argue that if every item of data entered into an automated system could be associated with an identifier unique to the individual to whom the data pertain, updating, merging, and linking operations would be greatly simplified and far less error-prone than they are today. Moreover, records could be used more intensively; administrative records indexed by Social Security number, for example, could also be used for certain types of research which require matching data on individuals from several different record systems.

To reap the full technical advantages of a standard identification scheme, it is necessary for each individual to supply the identifier

⁸ See, for example, Russell Ackoff, "Management Misinformation Systems," in Westin, *op. cit.*, pp. 264-271.

assigned to him every time he has contact with a record-keeping organization using it. This practice is already familiar to the clients of banks, credit-card services, and many other organizations that have developed their own standard schemes. What worries people is that the inconvenience to record-keeping organizations of having to devise their own numbering arrangements will encourage the adoption of a single universal scheme for use in all computer-based personal data systems. If this happens, organizations that share an interest in monitoring and controlling the behavior of some portion of the population will acquire an enlarged capacity to do so, since they will all be able to know when an individual has contact with any one of them. Fingerprints, for example, are the standard method used by the police to identify persons arrested for crimes. Fingerprinting assures accurate identification and may seem a reasonable way of dealing with criminal offenders, but it is a dubious model for other types of record-keeping organizations to follow.

It is, of course, a long step from having each individual identified in the same way in every data system to creating a giant national data bank of dossiers constructed from fragments of records on citizens in widely dispersed data systems. There would have to be some strong incentive for "putting it all together," and as we noted earlier, it is doubtful that even the dollar cost of doing so could be justified on any reasonable grounds. However, it is not necessary to build a giant national data bank to experience some of the effects of having one. There are already systems in operation which have some of the control capabilities that such a centralized dossier system would create.

One computer-based personal data system that came to our attention was a comprehensive health information system developed and maintained by an agency of the Department of Health, Education, and Welfare on an Indian reservation in the Southwest. Approximately 10,000 Indians living in the area have records in the system and another 4,000 have records in it but, for one reason or another, are not part of the active patient population. These 14,000 record subjects are, by and large, an economically dependent population with very serious health problems. Within the confines of the geographic area covered by the system—about the size of

Connecticut—they are also a highly mobile population, with each individual going by any one of several different names depending on circumstances.

The health facility consists of a combination of in-patient, out-patient, and field-clinic services. The purpose of its computer-based record-keeping system is to develop a complete, cradle-to-grave, medical dossier on each individual eligible to use the facility, so that all can benefit from a comprehensive diagnostic and treatment program that aims to control illness by preventing its occurrence, or by taking preemptive steps at the first sign of a medical problem.

The record-keeping system has three basic components: (1) an administrative one that notes and describes every contact each patient has with any segment of the health facility, including the "interdisciplinary" teams of doctors, nurses, and social workers who travel about administering tests and providing ambulatory health services; (2) a statistical-reporting one that attempts to observe fluctuations in the incidence of certain types of ailments and to pinpoint "high risk" groups needing special preventive attention; and (3) a "surveillance" one that consists of the recorded results of medical tests administered according to a schedule established by the health facility. The system is a little more than three years old. By the summer of 1972 it contained about 50 million characters of data, or approximately 3,500 characters per patient-record. It accommodates data in narrative as well as standard computer-accessible form.

The system is an elegant tool for addressing a complex set of social problems. It would be hard to argue that the patient population being cared for would be better off without the services the system makes possible. It is also apparent that knowing who an individual is, and the details of his medical history, can be of vital importance in treating patients, but the system has certain social control capabilities that should be noted nonetheless.

The surveillance component, for example, has the primary purpose of discovering incipient medical problems in individual patients. To do this effectively, each patient must be induced to comply with the health facility's testing schedule, and the health

data system can be used to encourage compliance. As long as a patient has no need for medical treatment, he can avoid the testing program. However, once he becomes a patient, for whatever reason, his record will be there at the doctor's fingertips showing all tests he has not had but should be persuaded to have before he leaves the field clinic or wherever it is that he has come to the medical facility's attention. In discussing a system serving such patently humane purposes, words like "control" and "coercion" may have an objectionable ring, but the coercive *potential* of the surveillance component, especially in some other area of application, is evident.⁹

In another environment, the statistical-reporting component of the system could also have potentially unsavory consequences for individuals. It is characteristic of modern organizations to single out "high risk" categories of people to whom the normal standards and rules do not apply. Often these high risk groups are identified from statistical studies of populations that use the services an organization offers. The consequences for any given individual exhibiting the characteristics of the high risk group may range from total exclusion (uninsurability) to being made eligible for special treatment (remedial education, free medical care). Although there is nothing intrinsically harmful in such practices, in dealing with human populations it is essential not to assume that any single member of a statistically defined group will necessarily behave in the way predicted for the group as a whole. Theoretically, the adverse consequences of "statistical stereotyping" can be avoided by permitting an individual to know that he has been labelled a risk and to contest the label as applied to him. However, depending on the circumstances—and particularly on the stake that an organization may have in being able to predict the behavior of each individual in its clientele—a lone individual could have considerable difficulty making his case.

Even the administrative record-keeping component of a comprehensive data system can have coercive effects. When the administrative part of the health data system was described to the Committee, repeated reference was made to the advantages of knowing that a patient has previously been treated for an emotional

⁹ A computer-based information system designed to control the population of a prison is described in Appendix F.

disorder when he shows up at a clinic claiming that he has accidentally scratched his wrist on a rusty nail. One hopes that his chances of being discharged after some bandaging and a tetanus shot are about the same as his chances of being committed for treatment as a potential suicide. But are they? Should they be? In some other record-keeping environment, could an individual depend on having someone equivalent to a trained medical practitioner available to make such a judgment?

Finally, it is important to note that the health data system has grown very rapidly, that elements like the "high risk" categorization were not present in the beginning, and that the health facility is now trying to improve its method of identifying patients for the purpose of updating and retrieving the information it maintains about them. In this particular situation, the Social Security number happens to be considered a poor identification device because many patients are thought to have more than one; but the patients also tend to have several different names, so the managers of the data system are trying to develop their own unique numbering scheme cross-referenced with all known "aliases" for each patient.

Scheduling, labelling, monitoring, improved methods of identifying records about individuals—these are being discussed in some quarters today as if they were mere tools for delivering services to people efficiently. In the health data system just described, the surveillance component is regarded as a way of providing preventive health care; of taking preemptive steps to halt the natural development of illnesses and conditions conducive to illness. It is hard to quarrel with those objectives, or for that matter with the objectives of a great many data systems now in operation or being planned. Should a national credit-card service be prohibited from using a sophisticated personal data system to prevent its card holders from going on irresponsible spending sprees?¹⁰ Should school districts be forbidden to use personal data systems to help prevent children from becoming delinquents?

These are difficult questions to answer. Often the immediate costs of not using systems to take preemptive action against

¹⁰ For a cogent description of how this is done, see James B. Rule, *Private Lives and Public Surveillance* (London: Allen Lane), 1973, especially Chapter 6. See also Robert A. Hendrickson, *The Cashless Society* (New York: Dodd, Mead & Company), 1972.

individuals can be estimated (in both dollars and predictable social disruption), while the long-term costs of increasing the capacity of organizations to anticipate, and thus to control, the behavior of individuals can be discussed only speculatively. One fact seems clear, however; systems with preemptive potential are typically developed by organizations, and groups of organizations, who see them primarily as attractive technological solutions to complex social problems. The individuals that the systems ultimately affect, the people about whom notations are made, the people who are being labelled and numbered, have, by comparison, a very weak role in determining whether many of these systems should exist, what data they should contain, and how they should be used.

The Net Effect on People

Today it is much easier for computer-based record keeping to affect people than for people to affect computer-based record keeping. This signal observation applies to a very broad range of automated personal data systems. When a machine tool produces shoddy products, the reaction of consumers (and of government regulatory agencies in some cases) is likely to give the factory managers prompt and strong incentives to improve their ways. This is much less likely to be the case when computerized record-keeping operations fail to meet acceptable standards.

There is some evidence that in commercial settings competition helps to prevent harmful or insensitive record-keeping practices, especially when a record-keeping organization (a bank, for instance) depends on continuous interaction with individual data subjects in order to keep its own records straight. It is also true that a number of schools and colleges have been forced to abandon automated registration and scheduling by determined student campaigns to fold, spindle, and mutilate. In governmental settings, however, the dissatisfied data subject usually has nowhere else to take his business and can even be penalized for refusing to cooperate. The result, of course, is that many organizations tend to behave like effective monopolies, which they are.

It is no wonder that people have come to distrust computer-based record-keeping operations. Even in non-governmental settings, an individual's control over the personal information that he

gives to an organization, or that an organization obtains about him, is lessening as the relationship between the giver and receiver of personal data grows more attenuated, impersonal, and diffused. There was a time when information about an individual tended to be elicited in face-to-face contacts involving personal trust and a certain symmetry, or balance, between giver and receiver. Nowadays an individual must increasingly give information about himself to large and relatively faceless institutions, for handling and use by strangers—unknown, unseen and, all too frequently, unresponsive. Sometimes the individual does not even know that an organization maintains a record about him. Often he may not see it, much less contest its accuracy, control its dissemination, or challenge its use by others.

In more than one opinion survey, worries and anxieties about computers and personal privacy show up in the replies of about one third of those interviewed. More specific concerns are usually voiced by an even larger proportion.¹¹ The public fear of a "Big Brother" system, in effect a pervasive network of intelligence dossiers, focuses on the computer, but it includes other marvels of twentieth-century engineering, such as the telephone tap, the wireless microphone, the automatic surveillance camera, and the rest of the modern investigator's technical equipment. Such worries seem naive and unrealistic to a data-processing specialist, but as in the case of campus protests against computerized registration systems, the apprehension and distrust of even a minority of the public can grossly complicate even a safe, straightforward data-gathering and record-keeping operation that may be of undoubted social advantage.

It may be that loss of control and confidence are more significant issues in the "computers and privacy" debate than the organizational appetite for information. An agrarian, frontier society undoubtedly permitted much less personal privacy than a modern urban society, and a small rural town today still permits less than a big city. The poet, the novelist, and the social scientist tell us, each in his own way, that the life of a small-town man, woman, or family is an open book compared to the more anonymous existence of

¹¹ See, for example, *A National Survey of the Public's Attitudes Toward Computers* (AFIPS-TIME, Inc.) 1971. This survey is discussed in Alan F. Westin and Michael A. Baker, *Databanks in a Free Society* (New York: Quadrangle Books), 1972, pp. 465-485.

urban dwellers. Yet the individual in a small town can retain his confidence because he can be more sure of retaining control. He lives in a face-to-face world, in a social system where irresponsible behavior can be identified and called to account. By contrast, the impersonal data system, and faceless users of the information it contains, tend to be accountable only in the formal sense of the word. In practice they are for the most part immune to whatever sanctions the individual can invoke.

As every man goes through life he fills in a number of forms for the record, each containing a number of questions. . . . There are thus hundreds of little threads radiating from every man, millions of threads in all. If these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialized as rubber bands, buses, trams and even people would all lose the ability to move, and the wind would be unable to carry torn-up newspapers or autumn leaves along the streets of the city. They are not visible, they are not material, but every man is constantly aware of their existence. . . . Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads.

Alexander Solzhenitsyn,
Cancer Ward

Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.

Justice Louis D. Brandeis,
Olmstead v. United States, 1928

III

Safeguards for Privacy

There is widespread belief that personal privacy is essential to our well-being—physically, psychologically, socially, and morally. Concern about the effects of computerized personal data systems centers on their threat to privacy. Safeguards must therefore focus on the protection of personal privacy.

The rationale for the safeguards that we will recommend is set forth in this chapter. In it we take account of existing legal constraints on the invasion of personal privacy through record keeping, and of the role that records play in the relationship between individuals and record-keeping organizations.

Personal Privacy, Record Keeping, and the Law

Some suggest that the risks presented by automated personal data systems call for a Constitutional amendment, or a general legislative enactment, which would clearly and with certainty establish personal privacy as an explicit legal right. Others, no less committed to the protection of personal privacy, contend that existing law will evolve naturally to meet whatever challenges to privacy may result from computer-based record-keeping practices. In the latter view, the enactment of an explicit, general right of personal privacy, whether Constitutionally or by statute, would not only provide no greater protection than is already latent in the common law of privacy, but also would create uncertainty and

confusion that the courts are ill-suited to resolve.

Although the Constitution of the United States does not mention a right to privacy, and only three State Constitutions (Alaska, California, and South Carolina) make explicit provision for a right of privacy, various aspects of personal privacy have been protected against government action by judicial interpretation of certain provisions of the Bill of Rights. The First Amendment guarantees free speech, a free press, and freedom of assembly and religion; the Third Amendment prohibits quartering soldiers in private homes; the Fourth Amendment prohibits unreasonable searches and seizures; the Fifth Amendment protects against compulsory self-incrimination; and the Ninth Amendment guarantees that rights not enumerated in the Constitution are retained by the people. Courts have construed these protections of the Bill of Rights to uphold the individual's right not to be coerced into revealing political, social, or philosophical beliefs, or private associations, unless national security or public order are at stake. The issues in many cases are clearly rooted in concerns for personal privacy, but the courts have articulated their decisions in terms of Bill of Rights guarantees. The Supreme Court, however, has recognized a right of privacy as the basis for protecting the freedom of individuals to practice contraception, to read or look at pornography at home, and to have an unwanted pregnancy terminated.

Courts have also developed principles in the common law to allow suits for invasion of privacy in various situations involving financial or reputational injury of one person by another. There is little evidence, however, that court decisions will, either by invoking Constitutional rights or defining common law principles, evolve *general* rules, framed in terms of a legal concept of personal privacy, that will protect individuals against the potential adverse effects of personal-data record-keeping practices. Indeed, there are many court decisions in which seemingly meritorious claims that could have been sustained by recognizing a right of privacy were denied because the courts would not permit such a right to override other legal considerations.

Although there is a substantial number of statutes and regulations that collectively might be called the "law of personal-data record keeping," they do not add up to a comprehensive and

consistent body of law. They reflect no coherent or conceptually unified approach to balancing the interests of society and the organizations that compile and use records against the interests of individuals who are the subjects of records.¹

The Federal Reports Act² and the so-called "Freedom of Information Act,"³ taken together, come as close as any enactments to providing a framework for *Federal* policy in this area. However, they are limited in application to agencies of the Federal government; they deal in a limited fashion with only two aspects of record-keeping practice—data collection and data dissemination; and they contain scant and potentially inconsistent protections for the interests of individual record subjects.

The Federal Reports Act requires that Federal agencies, with several significant exceptions, obtain concurrence from the Office of Management and Budget before collecting "information upon identical items, from ten or more persons." The Act was designed chiefly to help business enterprises. Its main purposes are to minimize the "burden" upon those required to furnish information to the Federal government; to minimize the government's data-collection costs; to avoid unnecessary duplication of Federal data-collection efforts; and to maximize the usefulness to all Federal agencies of the information collected. Although concern for the interests of individuals can be discerned in its administration, the Act itself makes no mention of personal privacy. It neither creates nor recognizes any rights for individuals with respect to the personal-data record-keeping practices of the Federal government.

The Freedom of Information Act mandates disclosure to the public of information held by the Federal government. It barely nods at the interest of the individual record subject by giving Federal agencies the authority to withhold personal data whose disclosure would constitute a clearly unwarranted invasion of privacy. The Act, however, is an instrument for disclosing information rather than for balancing the conflicting interests that surround the public disclosure and use of personal records. The Act permits

¹ Appendix G contains a review of law that bears on the collection, storage, use, and dissemination of information by the Department of Health, Education, and Welfare.

² 44 U.S.C. 3501-3511.

³ 5 U.S.C. 552.

exemption from mandatory disclosure for personal data whose disclosure would constitute a "clearly unwarranted invasion of personal privacy," but the agency is given total discretion in deciding which disclosures meet this criterion. The Act gives the data subject no way at all to influence agency decisions as to whether and how disclosure will affect his privacy.⁴

Many of the States have similarly broad "public records" or "freedom of information" statutes whose objective is to assure public access to records of State government agencies. Most of them, however, provide no exceptions from their general disclosure requirements in recognition of personal privacy interests. We discovered no State law counterparts to the Federal Reports Act.

By and large, one finds that record-keeping laws and regulations at all levels of government are limited and specific in their application. The requirements and prohibitions they impose apply to particular types of organizations, records, or record-keeping practices. They seldom go further than to stipulate that particular records shall be maintained and made accessible to the public, to particular officials, or for particular purposes, or that particular records shall be subject to confidentiality constraints. No body of statutory or administrative law establishes rights for individual record subjects or other rules of general application governing personal-data record-keeping practices, whether manual or automated.

Nor should we look to court decisions to develop such general rules. Courts can only decide particular cases; their opportunity to establish legal principle is limited by the nature of litigation arising from controversies between parties. Few cases that raise the broad issues posed by all personal-data record keeping have been brought before the courts, and fewer that focus those issues on computer-based systems. There are several possible explanations for this.

One possibility is that nobody has been hurt enough or has felt sufficiently aggrieved by current record-keeping practices to bring suit. Another is that record-keeping and data-processing practices are not an overt or well understood function of institutions,

⁴The privacy implications of the Freedom of Information Act and its application to computer-based record-keeping systems are discussed in Arthur R. Miller, *The Assault on Privacy* (Ann Arbor: University of Michigan Press), 1971, pp. 152-161.

whether governmental or private. Their adverse effects may not have been recognized. The individual affected may never discover that the root of his difficulties with an institution was some piece of information about him in a record. This is one reason for the section in the Fair Credit Reporting Act⁵ that requires than an individual be notified when an adverse action, such as denial of credit, insurance, or employment, is taken on the basis of a report from a consumer-reporting agency.

Still another possibility is that unless injury to the individual can be translated into reasonably substantial claims for damages, the individual ordinarily has little incentive to undertake a lawsuit. Few people can afford to bring suit against a well-defended organization solely for moral satisfaction.

Record-keeping practices have ancient and predominantly honorable traditions, as we have seen. Historically, their social utility has seldom been questioned. Only when record-keeping systems can be shown to have caused actual injury, to have created problems with serious Constitutional implications, or to be in conflict with clear statutory requirements, are courts likely to interfere with their operation. As a consequence, government data systems appear, under existing law, to be virtually immune to constraint through suits by individual data subjects; private-sector systems appear no less so. The personal-data record-keeping operations of private organizations are unlikely to give rise to Constitutional issues and are typically not subject to statutory requirements.⁶ The judicial process, in short, seems functionally ill-suited to initiating development of general common law rules relating to record-keeping practices.

The foregoing analysis leads us to conclude that the natural evolution of existing law will not protect personal privacy from the risks of computerized personal data systems. In our view the analysis also disposes of any expectation that enactment of a mere

⁵15 U.S.C. 1681-1681t (1970).

⁶The Fair Credit Reporting Act is a notable exception.

right of personal privacy would afford such protection.⁷ The creation of such a right without precise and elaborate definition of its intended significance would not overcome the obstacles in the judicial process that hinder recognition of personal privacy in relation to record keeping. The development of legal principles comprehensive enough to accommodate a range of issues arising out of pervasive social operations, applications of a complex technology, and conflicting interests of individuals, record-keeping organizations, and society, will have to be the work of legislative and administrative rule-making bodies.

A Redefinition of the Concept of Personal Privacy

Our review of existing law leads to the conclusion that agreement must be reached about the meaning of personal privacy in relation to records and record-keeping practices. It is difficult, however, to define personal privacy in terms that provide a conceptually sound framework for public policy about records and record keeping and a workable basis for formulating rules about record-keeping practices. For any one individual, privacy, as a value, is not absolute or constant; its significance can vary with time, place, age, and other circumstances. There is even more variability among groups of individuals. As a social value, furthermore, privacy can easily collide with others, most notably free speech, freedom of the press, and the public's "right to know."

Dictionary definitions of privacy uniformly speak in terms of seclusion, secrecy, and withdrawal from public view. They all denote a quality that is not inherent in most record-keeping systems. Many records made about people are public, available to anyone to see and use. Other records, though not public in the

⁷From this conclusion we should not be understood to be unaware of the potential significance of an unqualified right of personal privacy—either Constitutionally or by statute. We know of at least one instance in which the existence of such a right in a State constitution served as the basis for the State's Attorney General to deny access to certain public records whose disclosure was not explicitly provided for in the governing State statutes. We would support enactment of a right of personal privacy for many reasons, but not as the only or best way to protect personal privacy in computer-based record-keeping systems.

sense that anyone may see or use them, are made for purposes that would be defeated if the data they contain were treated as absolutely secluded, secret, or private. Records about people are made to fulfill purposes that are shared by the institution maintaining them and the people to whom they pertain. Notable exceptions are intelligence records maintained for criminal investigation, national security, or other purposes. Use of a record about someone requires that its contents be accessible to at least one other person—and usually many other persons.

Once we recognize these characteristics of records, we must formulate a concept of privacy that is consistent with records. Many noteworthy attempts to address this need have been made.

Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.⁸

...this is the core of the "right of individual privacy"—the right of the individual to decide for himself, with only extraordinary exceptions in the interests of society, when and on what terms his acts should be revealed to the general public.⁹

The right to privacy is the right of the individual to decide for himself how much he will share with others his thoughts, his feelings, and the facts of his personal life.¹⁰

As a first approximation, privacy seems to be related to secrecy, to limiting the knowledge of others about oneself. This notion must be refined. It is not true, for instance, that the less that is known about us the more privacy we have. Privacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves.¹¹

The significant elements common to these formulations are (1) that there will be some *disclosure* of data, and (2) that *the data*

⁸ Alan F. Westin, *Privacy and Freedom* (New York: Atheneum), 1967, p. 7.

⁹ *Ibid.*, p. 373.

¹⁰ Office of Science and Technology of the Executive Office of the President, *Privacy and Behavioral Research* (Washington, D.C., 1967), p. 8.

¹¹ Charles Fried, "Privacy," *The Yale Law Journal*, Vol. 77 (1968), p. 482.

subject should decide the nature and extent of such disclosure. An important recognition is that privacy, at least as applied to record-keeping practices, is not inconsistent with disclosure, and thus with use. The further recognition of a role for the record subject in deciding what shall be the nature and use of the record is crucial in relating the concept of personal privacy to record-keeping practices.

Each of the above formulations, however, speaks of the data subject as having a unilateral role in deciding the nature and extent of his self-disclosure. None accommodates the observation that records of personal data usually reflect and mediate relationships in which both individuals and institutions have an interest, and are usually made for purposes that are shared by institutions and individuals. In fact, it would be inconsistent with this essential characteristic of mutuality to assign the individual record subject a unilateral role in making decisions about the nature and use of his record. To the extent that people want or need to have dealings with record-keeping organizations, they must expect to share rather than monopolize control over the content and use of the records made about them.

Similarly, it is equally out of keeping with the mutuality of record-generating relationships to assign the institution a unilateral role in making decisions about the content and use of its records about individuals. Yet it is our observation that organizations maintaining records about people commonly behave as if they had been given such a unilateral role to play. This is not to suggest that decisions are always made to the disadvantage of the record subject; the contrary is often the case. The fact, however, is that the record subject usually has no claim to a role in the decisions organizations make about records that pertain to him. His opportunity to participate in those decisions depends on the willingness of the record-keeping organization to let him participate and, in a few instances, on specific rights provided by law.

Here then is the nub of the matter. Personal privacy, as it relates to personal-data record keeping must be understood in terms of a concept of mutuality. Accordingly, we offer the following formulation:

An individual's personal privacy is directly affected by the kind of disclosure and use made of identifiable information

about him in a record. A record containing information about an individual in identifiable form must, therefore, 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.

This formulation does not provide the basis for determining *a priori* which data should or may be recorded and used, or why, and when. It does, however, provide a basis for establishing procedures that assure the individual a right to participate in a meaningful way in decisions about what goes into records about him and how that information shall be used.

Safeguards for personal privacy based on our concept of mutuality in record-keeping would require adherence by record-keeping organizations to certain fundamental principles of fair information practice.

- *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 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 reasonable precautions to prevent misuse of the data.*

These principles should govern the conduct of all personal-data record-keeping systems. Deviations from them should be permitted only if it is clear that some significant interest of the individual data subject will be served or if some paramount societal interest can be clearly demonstrated; no deviation should be permitted except as specifically provided by law.

Mechanisms for Providing Safeguards

Many mechanisms have been suggested for providing safeguards against the potential adverse effects of automated personal-data systems. Those who believe a general right of personal privacy should be established, by Constitutional amendment or by statute, propose, in effect, that the courts should be the mechanism. Although we have concluded that a general right of privacy is not a reliable approach to achieving effective protection, the safeguards we recommend in the following chapters of this report would rely in part on the courts.

Some have proposed that there be a public ombudsman to monitor automated personal data systems, to identify and publicize their potential for adverse effects, and to investigate and act on complaints about their operation. We note with approval the efforts of the Association for Computing Machinery, and of many business firms and newspapers, to provide ombudsman service to the victims of computer errors. We believe the benefits of this approach are many and would like to see it extended to more systems. However, the ombudsman concept is basically remedial and will, therefore, work best in the context of established rights and procedures. Furthermore, the function is not well understood or widely accepted in America, and some observers feel it has severe limitations in the context of American legal, political, and administrative traditions.

The "strongest" mechanism for safeguards which has been suggested is a centralized, independent Federal agency to regulate the use of all automated personal data systems. In particular, it has been proposed that such an agency, if authorized to register or license the operation of such systems, could make conformance to specific safeguard requirements a condition of registration or

licensure. The number and variety of institutions using automated personal data systems is enormous. Systems themselves vary greatly in purpose, complexity, scope of application, and administrative context. Their possible harmful effects are as much a product of these features as of computerization alone. We doubt that the need exists or that the necessary public support could be marshalled at the present time for an agency of the scale and pervasiveness required to regulate all automated personal data systems. Such regulation or licensing, moreover, would be extremely complicated, costly, and might uselessly impede desirable applications of computers to record keeping.^{1 2}

The safeguards we recommend require the establishment of no new mechanisms and seek to impose no 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. They aim to create no obstacles to further development, adaptation, and application of a technology that, we all agree, has brought a variety of benefits to a wide range of people and institutions in modern society.

The proposed safeguards are intended to assure that decisions about collecting, recording, storing, disseminating, and using identifiable personal data will be made with full consciousness and consideration of issues of personal privacy—issues that arise from

^{1 2}These comments point up what we regard to be the deficiencies of a regulatory approach that would constitute a single Federal agency as the regulatory body. They are not intended to discourage the development of regulation in specific, limited areas of application of computer-based record-keeping systems. For example, where particular institutions or societal functions are already subject to regulation, e.g., public utilities, common carriers, insurance companies, hospitals, it well may be that an effective way to introduce and enforce safeguard requirements would be through the public agencies that regulate such institutions. Such an approach has been adopted with respect to the credit-reporting industry (see discussion, Chapter IV, p. 69).

Many municipal governments have been exploring regulatory or quasi-regulatory mechanisms for applying safeguard requirements to so-called "integrated municipal information systems." The efficacy of such mechanisms has not yet been demonstrated; however, we know of several that appear promising in conception. In addition, at both State and local government levels, efforts are being made to regulate the use of criminal justice information systems.

inherent conflicts and contradictions in values and interests. Our recommended safeguards cannot assure resolution of those conflicts to the satisfaction of all individuals and groups involved. However, they can assure that those conflicts will be fully recognized and that the decision-making processes in both the private and public sectors, which lead to assigning higher priority to one interest than to another, will be open, informed, and fair.

The safeguards we will recommend are intended to create incentives for institutions that maintain automated personal data systems to adhere closely to basic principles of fair information practice. Establishment of a legal protection against unfair information practice to embody the safeguard requirements described in Chapters IV, V, and VI, will invoke existing mechanisms to assure that automated personal data systems are designed, managed, and operated with due regard for protection of personal privacy. We intend and recommend that institutions should be held legally responsible for unfair information practice and should be liable for actual and punitive damages to individuals representing themselves or classes of individuals. With such sanctions institutional managers would have strong incentives to make sure their automated personal data systems did not violate the privacy of individual data subjects as defined.

Of greatest importance, from our point of view, the safeguards we will recommend give the courts a reliable and generally applicable basis for protecting personal privacy in relation to record keeping. The legal concept of fair information practice we recommend will obviate the need to search for new Constitutional doctrines or to invent ways of extending the existing common law of privacy to cover situations for which it is conceptually ill-suited.

The Costs of Safeguards

The safeguards we recommend will not be without costs, which will vary from system to system. The personal-data record-keeping practices of some organizations already meet many of the standards called for by the safeguards. The Social Security Administration, for example, maintains a record of earnings for each individual in the Social Security system, and each individual has the legal right to learn the content of his record. Procedures have been set up to

allow an individual to find out easily what is in his record and to have the record corrected if it is wrong. Disclosure of an individual's record outside the system is forbidden, except under certain limited circumstances prescribed by statute and regulation, and there are criminal penalties for unauthorized disclosure. An individual is given notice and opportunity for a hearing when the record is being changed at the initiative of the Social Security Administration. These protections are a normal part of Social Security administration and, in our view, demonstrate the feasibility of building such safeguards into any system when the system's managers are strongly committed to do so.

We believe that the cost to most organizations of changing their customary practices in order to assure adherence to our recommended safeguards will be higher in management attention and psychic energy than in dollars. These costs can be regarded in part as deferred costs that should already have been incurred to protect personal privacy, and in part as insurance against future problems that may result from adverse effects of automated personal data systems. From a practical point of view, we can expect to reap the full advantages of these systems only if active public antipathy to their use is not provoked.^{1 3}

The past two decades have given America intensive lessons in the difficulty of trying to check or compensate for undesirable side-effects stemming from headlong application and exploitation of complex technologies. Water pollution, air pollution, the annual highway death toll, suburban sprawl, and urban decay are all unanticipated consequences of the too narrowly conceived and largely unconstrained applications of technology. Hence, it is

^{1 3}In addition to maintaining and using records of personal information, computer technology is a tremendous new force for development in many ways. Already, for example, computers are controlling traffic on city streets and highway systems, and in the air; supplementing human judgment in making medical diagnoses; monitoring air pollution; predicting the weather; and even acting as surrogates for human decision makers in controlling large electrical power systems, industrial manufacturing processes, and high-speed rail transportation systems. Such computer applications do not typically require identifiable information about people. That which is required is limited and need be retained for only a short time. Thus the social risks from computer systems such as these are beyond the scope of this report.

essential now for organizational decision makers to understand why they should be sensitive to issues of personal privacy and not permit their organizations unilaterally to adopt computer-based record-keeping practices that may have adverse effects on individuals. They must recognize where conflicts are likely to arise between an individual's desire for personal privacy and an organization's record-keeping goals and behavior. They must recognize that although individuals and record-keeping organizations do have certain shared purposes, they also have other purposes—some of which are mutual, though not perceived as such, and some of which can be in direct conflict.

Record-keeping organizations must guard against insensitivity to the privacy needs and desires of individuals; preoccupied with their own convenience or efficiency, or their relationships with other organizations, they must not overlook the effects on people of their record-keeping and record-sharing practices. They have the power to eliminate misunderstanding, mistrust, frustration, and seeming unfairness; they must learn to exercise it.

*I know everybody's income and what everybody earns;
And I carefully compare it with the income-tax returns;*

*To everybody's prejudice I know a thing or two;
I can tell a woman's age in half a minute—and I do!*

*Yet everybody says I am a disagreeable man!
And I can't think why!*

King Gama in Gilbert and Sullivan's
Princess Ida

IV

Recommended Safeguards for Administrative Personal Data Systems

Our inquiry has led us to distinguish two categories of personal data systems that deserve separate attention in developing safeguards. One consists of administrative systems; the other of statistical-reporting and research systems. The essential distinction between the two categories is functional. An administrative personal data system maintains data on individuals for the purpose of affecting them directly as individuals—for making determinations relating to their qualifications, character, rights, opportunities, or benefits. A statistical-reporting or research system maintains data about individuals exclusively for statistical reporting or research, and is not intended to be used to affect any individual directly.¹

¹In our brief review of the history of record keeping in Chapter I, we took note of the origins and existence of *intelligence* records. These should be thought of as a type of administrative personal data system, since intelligence records are maintained about people for the purpose of affecting them directly as individuals. We have not, however, examined intelligence record-keeping systems as such, and it was not with such systems in mind that we developed the safeguard recommendations set forth in this chapter. At the end of the chapter, we have included a brief statement about the application of our safeguards to intelligence records.

This chapter contains general recommendations for all personal data systems and safeguard requirements for administrative personal data systems used as such. Chapter V contains additional safeguard requirements for statistical-reporting and research applications of administrative systems. Systems maintained *exclusively* for statistical reporting or research and safeguard requirements for them are addressed in Chapter VI.

Although our specific charge has been to analyze problems of *automated* systems, our recommendations could wisely be applied to all personal data systems, whether automated or manual. Computer-based systems magnify some record-keeping problems and introduce others, but no matter how data are stored, any maintenance of personal data presents some of the problems discussed in Chapters II and III. Moreover, the distinction between an automated and a non-automated system is not always easy to draw; requiring safeguards for all personal data systems eliminates the need to rule on ambiguous cases. Uniform application of safeguards to all systems will also facilitate conversion from manual to automated data processing when it does occur.

We define an *automated personal data system* as a collection of records containing personal data that can be associated with identifiable individuals, and that are stored, in whole or in part, in computer-accessible files. Data can be “associated with identifiable individuals” by means of some specific identification, such as name or Social Security number, or because they include personal characteristics that make it possible to identify an individual with reasonable certainty. “Personal data” include all data that describe anything about an individual, such as identifying characteristics, measurements, test scores; that evidence things done by or to an individual, such as records of financial transactions, medical treatment, or other services; or that afford a clear basis for inferring personal characteristics or things done by or to an individual, such as the mere record of his presence in a place, attendance at a meeting, or admission to some type of service institution. “Computer-accessible” means recorded on magnetic tape, magnetic disk, magnetic drum, punched card, or optically scannable paper or film. A “data system” includes all processing operations, from initial collection of data through all uses of the data. Data recorded on

questionnaires, or stored in microfilm archives, are considered part of the data system, even when the computer-accessible files themselves do not contain identifying information.

Consistent with the rationale set forth in Chapter III, 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. (Safeguard requirements for administrative personal data systems are set out below; those for statistical-reporting and research systems will be found in Chapter VI.)
- 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. Labor unions, for example, might find the application of the safeguards to employee records an appropriate issue in collective bargaining.

Establishing Automated Personal Data Systems

We were not charged with developing criteria for determining when and for what purposes to establish personal data systems. It is doubtful that any such criteria are feasible or warranted. Our inquiry, however, has prompted us to make cautionary observations to those who must decide whether, when, and how to establish automated personal data systems.

The general proposition that records and record-keeping systems are desirable and useful does not necessarily apply to every system. Some data systems appear to serve no clearly defined purpose; some appear to be overly ambitious in scale; others are poorly designed; and still others contain inaccurate data.

Each time a new personal data system is proposed (or expansion of an existing system is contemplated) those responsible for the activity the system will serve, as well as those specifically charged with designing and implementing the system, should answer explicitly such questions as:

What purposes will be served by the system and the data to be collected?

How might the same purposes be accomplished without collecting these data?

If the system is an administrative personal data system, are the proposed data items limited to those necessary for making required administrative decisions about individuals as individuals?

Is it necessary to store individually identifiable personal data in computer-accessible form, and, if so, how much?

Is the length of time proposed for retaining the data in identifiable form warranted by their anticipated uses?

A careful consideration of questions such as these might avert the establishment of some systems. Even if a proposed system survives a searching examination of the need for it, the very process should at least suggest limitations on the collection and storage of data.

Formalized administrative procedures and requirements should be followed to assure that questions about the purposes, scope, and

utility of systems are raised and confronted before systems are established or enlarged. Members of the public should also have an opportunity to comment on systems before they are created.

It is especially important that such procedures be followed whenever data collection requirements, imposed by any Federal department or agency on States, other grantees, or regulated organizations, are likely to result in the creation or enlargement of personal data systems. In our view, any such data collection requirement should be established by regulations adopted after the public has been given an opportunity to comment, rather than by less formal means, such as program guidelines or manuals. Adoption of a regulation also forces a Federal agency to go through a formal process of internal justification and executive review. In the case of Federal data-collection requirements, the notice of any proposed regulation should contain a clear explanation of why each item of data is to be collected and why it must be collected and stored in identifiable form, if such is proposed.

The Safeguard Requirements

An automated personal data system should operate in conformity with safeguard requirements that, as stated above, should be enacted as part of a code of fair information practice. It is difficult to formulate safeguard requirements that will assure, in every system, an appropriate balance between the interest of the individual in controlling information about himself and all other interests—institutional and societal. However, because the safeguards we recommend are so basic to assuring fairness in personal data record keeping, any particular system, or class of systems, should be exempted from any one of them only for strong and explicitly justified reason.

If organizations maintaining personal data systems are left free to decide for themselves when and to what extent to adhere fully to the safeguard requirements, the aim of establishing by law a basic code of fair information practice will be frustrated. Thus, exemptions from, or modifications of, any of the safeguard requirements should be made only as specifically provided by statute, and there should be no exemption or modification unless societal interest in allowing it can be shown to be clearly paramount

to the interest of individuals in having the requirement imposed. "Societal interest," moreover, should not be construed as equivalent to the convenience or efficiency of organizations that maintain data systems, the preference of a professional group, or the welfare of individual data subjects as defined by system users or operators. Existing policies that guide the handling of personal data should not be uncritically accepted or reaffirmed. Nor should the basic "least common denominator" quality of the safeguards discourage law-making bodies, or organizations maintaining personal data systems, from providing individuals greater protection than the safeguards offer. Existing laws or regulations that provide protections greater than the safeguards should be retained; those that provide less protection should be amended to meet the standards set by the safeguards.

SAFEGUARD REQUIREMENTS FOR ADMINISTRATIVE PERSONAL DATA SYSTEMS

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.

All other safeguard requirements for administrative personal data systems have been formulated to apply only to *automated* systems. As suggested earlier, the safeguards would wisely be applied to all personal data systems that affect individuals directly, whether or not they are automated. If this is not done, however, it is necessary to assure that individuals about whom an organization maintains records of personal data, which are not part of an automated system, will be protected in the event that personal data from those records are transferred to automated systems. Requirement I.A. is intended to provide such protection by requiring that transfers of personal data to automated systems not subject to the safeguard requirements be made only with the informed consent of the individuals to whom the data pertain.

The requirement is formulated so as not to apply to transfers of personal data that are not in individually identifiable form, e.g., for statistical reporting. (Transfers of individually identifiable data to automated systems used exclusively for statistical reporting and research are covered in Chapter VI, p. 97.)

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;

The obligation to identify a person responsible for the system is intended to provide a focal point for assuring compliance with the safeguard requirements and to guarantee that there will be someone with authority to whom a dissatisfied data subject can go, if other methods of dealing with the system are unsatisfactory. Systems that involve more than one organization may present special problems in this respect, and must be carefully designed to assure that a data subject is not shuffled from one organization to another when he seeks to assert his rights under these 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;

This requirement takes account of the fact that the actions of many people, with diverse responsibilities and functions located in different parts of an organization, affect the operations of an automated personal data system. Often these people lack a common understanding of the possible consequences for the system of their separate actions. If an organization is to comply fully and efficiently with the safeguard requirements, its employees will have to be made thoroughly aware of all the rules and procedures the organization has established to assure compliance.

- (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;

The employees of an organization must not be penalized for attempting to prevent or expose violations of the safeguard requirements. Organizations maintaining systems must assure their employees that no harm will come to them as a consequence of bringing evidence of poor practice or willful abuse to the attention of parties who are willing and prepared to act on it.

A personal-data record-keeping system is often one of the least visible aspects of an organization's operations. Organization managers are sometimes ignorant of important facets of system operations, and individual clients or beneficiaries often do not perceive how their difficulties in dealing with an organization may stem from its record-keeping practices. Furthermore, systems tend to be designed, developed, and operated by sizable groups of specialists, no one of whom has a detailed understanding of how each system works and of all the ways in which it can be abused. This diffusion of responsibility, and of practical knowledge of system characteristics, makes the integrity of computer-based record-keeping systems especially dependent on the probity of system personnel. Efforts by associations of data processing specialists to gain nationwide adherence to a code of professional ethics attest to the importance of this aspect of system operations.

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

The purpose of requirement (4) is to assure that an organization maintaining an automated personal data system takes appropriate security precautions against unauthorized access to data in the system, including theft or malicious destruction of data files.

- (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 himself be transferred to another system or organization;

Requirement (5) is intended to provide protection against any additional risks to data security resulting from transfer of data from one system to another, or from the establishment of regular data linkages between systems. To comply with this requirement, an organization would have to be able to demonstrate that it had carefully followed procedures deliberately designed to assure that the security conditions for a data transfer, including transmission facilities and the data security features and access limitations of the system receiving the data, conform to specified expectations of the transferring organization and its data subjects. In combination with safeguard requirement III(3) (pp. 61-62, below), which requires an organization to obtain the informed consent of individual data subjects before permitting data about them to be put to uses that exceed their reasonable expectations, this requirement would, for example, prevent the sale of data files by one organization to another without the consent of the data subjects if the security features and access limitations of the purchasing organizations were such as to open the possibility of uses not anticipated by the data subjects. The exception in requirement (5) is intended to accommodate the possibility that an individual may need or want his record, or data therefrom, to be made available to another organization even though such transfer may entail risks of security or access that the transferring organization would not undertake or permit, and could not, consistent with this safeguard.

(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;

This requirement will contribute significantly to an organization's capacity to detect improper dissemination of personal data. It is not intended to include ordinary system housekeeping entries, such as updating of files, undertaken in the course of normal maintenance by system personnel. To facilitate its compliance with requirement III(4) (p. 62, below), an organization should consider assuring that records of access to and use of data are part of, or are easily associable with, the records of individuals that are accessed and used.

(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.

Requirements (7) and (8) are intended to reduce the number of instances in which individuals are adversely affected by poorly conceived, poorly executed, or excessively ambitious uses of automated personal data systems. Because specific deficiencies in individual records will constitute evidence that requirement (7) has been violated, the effect of the requirement will be to make an organization as alert to isolated errors as it is to sources of recurring errors. To assure alertness, giving high priority to periodic retraining of system personnel and the suitability of their working conditions is essential. In addition, the organization may find that regular evaluation is needed of its data collection procedures and of the accuracy with which data are being converted into computer-accessible form. If particular data are being reproduced for use by another system or organization, steps may also have to be taken to apprise the receiving organization of subtle pitfalls in interpreting the data.

Requirement (7) will discourage organizations from attempting to handle more data than they can adequately process and should also reduce the likelihood that computer-based "dragnet" operations will injure, embarrass, or otherwise harrass substantial numbers of individuals. Requirement (8) will promote the development of data-purging schedules that reflect the reasonable useful life of each category of data. Although the requirement would not prohibit the retention of data for archival purposes, it would assure that obsolete data are not available for routine use.

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.

The requirement for announcing the intention to create or enlarge a system stems from our conviction that public involvement is essential for fully effective consideration of the pros and cons of establishing a personal data system. Opportunity for public involvement must not be limited to actual or potential data subjects; it should extend to all individuals and interests that may have views on the desirability of a system.

We have not specified a uniform mechanism for giving notice, but rather expect all reasonable means to be used. In the Federal government, we would expect at least formal notice in the *Federal Register* as well as publicity through other channels, including mailings and public hearings. We would expect State and local governments to use whatever comparable mechanisms are available to them. For other organizations maintaining or proposing system arrangements such as newspaper advertisements may be appropriate. Whatever methods are chosen, an organization must have copies of its notices readily available to anyone requesting them.

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;

This requirement is intended to discourage organizations from probing unnecessarily for details of people's lives under circumstances in which people may be reluctant to refuse to provide the requested data. It is also intended to discourage coercive collection of personal data that are to be used exclusively for statistical reporting and research. (Secondary statistical-reporting and research applications of administrative personal data systems are the subject of Chapter V.)

- (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;

We considered having this requirement provide that an individual be informed that he is a data subject, whether or not he inquires. It seems to us, however, that such a requirement could be needlessly burdensome to some organizations, particularly if the character of their operations makes it likely that an individual will know that he is the subject of data in one or more systems—for example, systems that mail their customers monthly statements. Furthermore, since our objective is to specify a set of fundamental “least common denominator” standards of fair information practice, we concluded that it would be sufficient to guarantee each individual the right to ascertain whether he is a data subject when and if he asks to know.

We would, however, urge that organizations take the initiative to inform individuals voluntarily that data are being maintained about them, especially if it seems likely that the individuals would not be made fully aware of the fact as a consequence of normal system operations. For example, in systems where individuals become data subjects as a consequence of providing data about themselves in an application, the form could describe the records that will be maintained about them.

This requirement affords an individual about whom data are maintained in a system the right to be informed, and the right to obtain a copy of data, only if he may be affected individually by any use made of the system. For example, employees about whom earnings data are maintained in individually identifiable form in records kept by their employers would have these rights, but individuals appearing collaterally in records, such as an employee's dependents or character references, would have the rights afforded by this requirement only if they could be affected by the uses made of the records in which they appear.

We recognize that the right of an individual to have full access to data pertaining to himself would be inconsistent with existing practice in some situations. The medical profession, for example, often withholds from a patient his own medical records if knowledge of their content is deemed harmful to him; school records are sometimes not accessible to students; admission to schools, professional licensure, and employment may involve records containing third-party recommendations not commonly made available to the subject.

As indicated earlier (pp. 52-53, above), exemption from any one of the safeguard requirements should be only for a strong and explicitly justified reason. Thus, existing practices restricting an individual's right to obtain data pertaining to himself should be continued only if an exemption from the requirement of full access is specifically provided by law.

Reassessment of existing practices that deprive individuals of full access to data recorded about themselves will be one of the most significant consequences of establishing safeguard requirement III (2). Many organizations are likely to argue that it is not in the interest of their data subjects to have full access. Others may oppose full access on the grounds that it would disclose the content of confidential third-party recommendations or reveal the identity of their sources. Still others may argue that full access should not be provided because the records are the property of the organization maintaining the data system. Such objections, however, are inconsistent with the principle of mutuality necessary for fair information practice. No exemption from or qualification of the right of data subjects to have full access to their records should be granted unless there is a clearly paramount and strongly justified societal interest in such exemption or qualification.

If an organization concludes that disclosing to an individual the *content* of his record might be harmful to him, it can point that out, but if the individual persists in his request to have the data, he should, in our view be given it. The instances in which it can be convincingly demonstrated that there is paramount societal interest in depriving an individual of access to data about himself would seem to be rare.

Similarly, we cannot accede in general to the claim that the *sources* of recorded comments of third parties should be kept from a data subject if he wants to know them. Disclosure to the data subject of the sources of such comments may be difficult for organizations that have promised confidentiality. Modifying the data subject's right of access in order to honor past pledges may be necessary. However, the practice of recording data provided by third parties, with the understanding that the identities of the data providers will be kept confidential, should be continued only where there is a strong, clearly justified societal interest at stake. Elementary considerations of due process alone cast grave doubt on the propriety of permitting an organization to make a decision about an individual on the basis of data that may not be revealed to him or that have been obtained from sources that must remain anonymous 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;

This requirement is intended to deal with one of the central issues of fair information practice—controlling the use of personal data. Assume that a system maintains no more personal data than reasonably necessary to achieve its purposes. Assume further that its purposes are well understood and accepted by the individuals about whom data are being maintained, and that all data in the system are accurate, complete, pertinent, and timely. The question of how data in the system are actually used still remains.

Because an individual can be adversely affected even by accurate data in well-kept records, the use of personal data in a system should be held to standards of fairness that minimize the risk that an individual will be injured as a consequence of an organization's

permitting data about him to be used for purposes that differ substantially from whatever uses he has been led to expect. The public notice called for by safeguard requirement *II* (pp. 57-58, above) is intended to assure that when an individual first becomes a data subject, he will be able to understand the purposes of the system and the types of uses to which data about him will be put. If, however, an organization expands the previously announced purposes of the system, or enlarges the range of permissible uses of data in identifiable form, it must not only revise its public notice for the system, but also must obtain the prior consent of all existing data subjects.

The objective of requirement *III(3)*, in short, is to make it possible for individuals to avoid having data about themselves used or disseminated for purposes to which they may seriously object. The requirement applies to all new types of uses, whether they will be made by the system that initially collected that data or by some other system or organization to which data are to be transferred. Thus it applies (as noted on p. 56, above) to uses that may result from the transfer to data to a system whose security features and access limitations open the possibility of uses not anticipated by the data subjects.

(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;

This requirement will guarantee the individual an opportunity to find out exactly how and why data about him have been used, and by whom. It provides this right for an individual only when he makes a request; a general rule requiring an organization to take the initiative in all cases to inform an individual how data about him have been used would often not serve any useful purpose, and might lead, for example, to periodic mass mailings to inform individuals of uses of which they are already aware. Nonetheless, there may be instances when data subjects will want to be informed on a regular basis about particular types of data use. It is the intent of this safeguard that an organization provide such service when an individual requests it.

Coupled with requirement *I(6)* (p. 56, above) this requirement would also afford individuals the opportunity to advise those to whom records about them have been disseminated of any corrections, clarifications, or deletions that should be made.

(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;

“Compulsory legal process” includes demands made in the form of judicial or administrative subpoena and any other demand for data that carries a legal penalty for not responding. It should be the responsibility of the person or organization that seeks to obtain data by compulsory legal process to notify the data subject of the demand and to provide evidence of such notification to the system. In instances when it may be more practicable for the system to give notice of the demand to the data subject, the cost of doing so should be borne by the originator of the demand.

The intent of requirement (5) is to assure that an individual will know that data about himself are being sought by subpoena, summons, or other compulsory legal process, so as to enable him to assert whatever rights he may have to prevent disclosure of the data.

(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.

It is not the intent of this requirement in any way to relieve an organization of the obligation to maintain data in accordance with requirement *II(8)* (p. 57, above). Rather, in combination with requirement *II(8)*, it is expected to give an organization maintaining a system strong incentives to investigate and act upon any claim by an individual that data recorded about him are incorrect, insufficient, irrelevant, or out-of-date. The provision for obtaining

injunctions included in the Code of Fair Information Practice (p. 50, above) will enable individuals to seek court orders for corrective action in regard to their records.

Relationship of Existing Laws to the Safeguard Requirements

As we stated earlier in this chapter, 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. We have not attempted an exhaustive inventory of existing Federal and State statutes that may need to be amended to bring them into conformity with the safeguards, but in the course of our work we have identified two Federal statutes in regard to which we have specific recommendations.

FREEDOM OF INFORMATION ACT

The Federal Freedom of Information Act² has a disturbing feature that could be eliminated by means of an amendment quite in keeping with the primary purpose of the Act. As noted in Chapter III, the main objective of the Freedom of Information Act is to facilitate public access to information about how the Federal government conducts its activities. The Act contains a broad requirement that information held by Federal agencies be publicly disclosed. Nine categories of information are specifically exempted from the Act's mandatory disclosure requirement. For seven of the nine, moreover, disclosure is not prohibited or otherwise constrained by the Act, and the decision not to disclose is left entirely to the discretion of the agency holding the information. The agency is completely free to decide whether it will comply with a request that it disclose information falling within any of the seven exemptions.³

² 5 U.S.C. 552 (1970).

³ The remaining two exemptions refer to information that is: "specifically required by Executive order to be kept secret in the interest of the national defense or foreign policy;" and "specifically exempted from disclosure by statute." Legal prohibitions against disclosure of information in these two categories are not affected by the Act.

Of the seven discretionary exemptions, those that offer the most likely basis for an agency to withhold *personal* data from the public are:

trade secrets and commercial or financial information obtained from a person and privileged or confidential;

personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy; and

investigatory files compiled for law enforcement purposes except to the extent available by law to a party other than an agency.

The Act's failure to provide for data-subject participation in a decision by an agency to release personal data requested under the Act is inconsistent with safeguard requirement *III(3)* (p. 61, above) which calls for an individual's consent to any unanticipated use of data about himself in an administrative automated personal data system. Enactment of this requirement would necessitate modification of the Freedom of Information Act to give the data subject a voice in agency decisions about public disclosure of information covered by the Act, whenever such disclosure is not within the reasonable expectations of individuals about whom a Federal agency maintains data in an automated system.

As we see it, an agency that is the custodian of personal data about an individual should not have unilateral discretion to decide to grant a request for public disclosure of such data, especially if the data fall within one of the exempted categories under the Freedom of Information Act. The data custodian should have to obtain consent from the data subject before releasing identifiable personal data about him from an administrative automated personal data system, except in cases where making the requested disclosure without the individual's consent is within the stated purposes of the system as specifically required by a statute. We expect such cases to be few.

Accordingly, 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 exempt-

ed-category data about him, unless the disclosure is within the purposes of the system as specifically required by statute. Pending such amendment of the Act, we further recommend that all Federal agencies provide for obtaining the consent of individuals before disclosing exempted-category personal data about them under the Freedom of Information Act.

If the Act were so amended, its purpose of protecting the public's "right to know" about the activities of the Federal government would be brought into a better balance with the no less important public purpose of protecting the personal privacy of individuals who are the subjects of data maintained in the automated personal data systems of the Federal government. There may be other areas of conflict between the safeguard requirements and the Freedom of Information Act. The Act should be given a thorough reappraisal with a view to formulating additional amendments needed to accommodate the safeguard requirements. An amended Freedom of Information Act and the Code of Fair Information Practice we have proposed would, in combination, provide an improved statutory framework within which to resolve the unavoidable conflicts between personal privacy and open government.

FAIR CREDIT REPORTING ACT⁴

The Fair Credit Reporting Act is the first Federal statute regulating the vast consumer-reporting industry. Its basic purpose, as stated in the Act, is

to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy.

The consumer-reporting industry is comprised of credit bureaus, investigative reporting companies, and other organizations whose business is the gathering and reporting of information about individuals for use by others in deciding whether individuals who are the subject of such reports qualify for credit, insurance, or employment. Consumer-reporting agencies typically operate what

⁴15 U.S.C. 1681-1684t.

we have called administrative personal data systems, many of which contain large quantities of intelligence-type data. Increasingly, these systems are being computerized.

The Fair Credit Reporting Act requires consumer-reporting agencies to adopt reasonable procedures for providing information about individuals to credit grantors, insurers, employers and others in a manner that is fair and equitable to the individual with regard to confidentiality, accuracy, and the proper use of such information. It also places requirements on users of consumer reports and consumer-investigative reports.

The chief requirements imposed by the Act include the following:

Accuracy of Information

Consumer-reporting agencies must follow reasonable procedures in preparing reports to assure maximum possible accuracy of the information concerning the individual about whom the report is prepared. The effect of this requirement extends to all the data gathering, storing, and processing practices of an agency.

Obsolete Information

Certain items of adverse information may not be included in a consumer report after they have reached specified "ages" (except in connection with credit and life insurance transactions of \$50,000 or more and employment at an annual salary of \$20,000 or more) viz.: bankruptcies—14 years; suits and judgments—7 years; paid tax liens—7 years; accounts placed for collection or written off—7 years; criminal arrest, indictment, or conviction—7 years; any other adverse information—7 years.

Limited Uses of Information

A consumer-reporting agency may furnish a consumer report about an individual to be used for the following purposes and no other:

- in response to a court order;
- in accordance with written instructions of the individual to whom it relates;
- to determine the individual's eligibility for (i) credit or insurance to be used for personal, family, or household purposes, (ii) employment, including promotion, reassignment or retention

as an employee; or (iii) a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status;

- to meet a legitimate business need for a business transaction involving the individual.

A consumer-reporting agency must take all steps necessary to insure that its reports will be used only for the above purposes.

Notices to Individuals

Whenever credit, insurance, or employment is denied, or the charge for credit or insurance is increased, wholly or partly because of information in a report from a consumer-reporting agency, the user of the report must notify the individual affected and supply the name and address of the agency that made the report.

Whenever a consumer-reporting agency reports public record information about an individual which may adversely affect his ability to obtain employment, it must notify the individual that it is doing so, including the name and address of the person to whom the information is reported.

Whenever an investigative report (obtaining information through personal interviews with neighbors, friends, associates, or acquaintances) is to be prepared about an individual, he must be so notified in advance unless the report is for employment for which the individual has not applied.

Individual's Right of Access to Information

An individual about whom an investigative report is being prepared has the right, upon his request, to be informed of the nature and scope of the investigation.

An individual has the right, upon his request, and proper identification, to be clearly, accurately, and fully informed of: (i) the nature and substance of all information, except medical information, about him in the files of a consumer-reporting agency; (ii) the sources of such information, except sources of information obtained solely for an investigative report; and (iii) recipients of consumer reports furnished about the individual, within 2 prior years for employment purposes and within 6 prior months for any other purpose. (The individual has this right whether or not adverse action has been taken.)

Whenever credit is denied, or the charge for it increased, wholly or partly because of information obtained from a source other than a consumer-reporting agency, the individual affected has the right, upon his request, to learn the nature and substance of the information directly from its user.

Individual's Right to Contest Information

If an individual disputes the accuracy or completeness of information in a file maintained about him by a consumer-reporting agency, the agency must reinvestigate and record the current status of that information, or delete the information if it is found to be inaccurate or cannot be reverified. If the reinvestigation does not resolve the dispute, the individual has the right to file a brief statement explaining the dispute; and the agency must, in any subsequent report containing the disputed information, note the dispute and provide at least a clear summary of the individual's statement.

One reason for describing the Fair Credit Reporting Act in such detail is to illustrate the care with which the Congress has responded to the need it found to protect individuals from the adverse effects of unfair information practices in the consumer-reporting industry. Although the Congress adopted a regulatory approach in this Act,⁵ it constitutes a strong precedent for our recommended Code of Fair Information Practice. In regulating the practices of both consumer-reporting agencies and the users of their reports, the Act, in effect, imposes many of the safeguard requirements we recommend.

The chief reason for presenting the Fair Credit Reporting Act, however, is to illustrate the point that existing laws that provide greater protection for individuals than our safeguards offer should be retained, while laws that provide less protection should be amended to meet the standards set by the safeguards. Section 606(a) of the Fair Credit Reporting Act, 15 U.S.C. 1681d(a), for example, requires that an individual be notified that an investigative report is being prepared about him before work on it is begun, whereas safeguard requirement III(2) (p. 59, above) gives an individual the right to be informed that he is the subject of a record only if he asks to know. In this instance, the Act's requirement, responsive to the particular circumstances of the consumer-reporting industry, provides the individual with greater protection than our safeguard and should be retained.

⁵ The Federal Trade Commission has the basic responsibility for enforcing the Act, but where specific types of institutions are already regulated (for other purposes) by other agencies, those agencies are charged with enforcing the Act; e.g., the Comptroller of the Currency (national banks), the Federal Reserve Board (member banks of the Federal Reserve Systems other than national banks), the Interstate Commerce Commission (common carriers), and the Civil Aeronautics Board (air carriers).

Conversely, safeguard requirement *III(2)*, which also guarantees an individual the right to see and obtain copies of data about him, provides more protection for individuals than Section 609(a) of the Fair Credit Reporting Act, 15 U.S.C. 1681g(a). Under the Act's requirement the individual is entitled to be fully informed by a consumer-reporting agency of the content of his record (except medical information and the sources of investigative information), but he is not entitled to see, copy, or physically possess his record. When an individual goes to a consumer-reporting agency to determine what information it has on him, the contents of the record must be read to him, but he must take the agency's word that it is telling him about all information in the record, and about all sources and recipients thereof. We understand that individuals have found this arrangement generally unsatisfactory, and further, that as the proportion of "sensitive" or adverse personal data in a record increases, compliance with the full disclosure requirement tends to diminish.

To bring Section 609(a) more in line with the protection afforded individuals by safeguard requirement *III(2)*, and thus to achieve the objective of the Fair Credit Reporting Act more fully, we recommend 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. The choice between inspecting and copying should be left to the individual, and any charge for having copies made should be nominal.

We further recommend that the exceptions from disclosure to the individual now authorized by the Fair Credit Reporting Act for medical information and sources of investigative information should be omitted. It is a disturbing thought that an investigative consumer-reporting agency may have a record of medical information that the individual cannot know about or challenge. We realize that in Section 603(f) of the Fair Credit Reporting Act, 15 U.S.C. 1681a(f), "consumer reporting agencies" is defined broadly enough to apply to some organizations that are customary and appropriate repositories of medical information. However, nothing in the Act should warrant the inference that every type of organization falling within the umbrella definition of "consumer reporting agencies" may, with impunity, conceal from an individual the fact that it is gathering, recording, and reporting medical information about him.

We have explained our skepticism about the propriety of utilizing anonymous data sources when determinations about an individual's character, qualifications, rights, opportunities, or benefits are being made. Moreover, we find no strong societal interest in having an individual routinely denied credit, insurance, or employment on the basis of information provided by any source that must be kept secret from him.⁶

A Note on Mailing Lists

The use of automated personal data systems to generate mailing lists deserves special comment. Ordinarily such use entails no perceptible threat to personal privacy. Even among individuals who strongly object to receiving quantities of so-called "junk mail," most would probably concede that their objections are not founded on any substantial claim that personal privacy has been invaded. Indeed, it is hard to see how the mere delivery of an item of mail to an individual, even though it is addressed to him by name, in itself entails an offensive or harmful disclosure or use of personal data.

More important than the end use of the mailing list itself is the question of the original source of the personal data from which the list was originally assembled. In most cases, commercial mailing lists are made up of names and addresses gathered during the course of commercial transactions. In the most typical case, buying an item through the mail assures that the buyer's name will be added to the list of a commercial dealer in names, and that the list will in turn be sold, rented, and traded through a chain of further commercial mailers. This exploitation of names may occasionally be irritating, but there is little potential for substantial disclosure of closely held personal information, since nothing beyond name and address was probably revealed in the first place.

A more serious threat to personal privacy arises when mailing lists are compiled from sources that have nothing to do with commercial interests—the membership list of a professional society,

⁶Experience under the Fair Credit Reporting Act should be carefully assessed to identify other amendments necessary to assure the effectiveness of its intended protections for individuals. For an analysis of deficiencies of the Act, see "Protecting the Subjects of Credit Reports," *The Yale Law Journal*, Vol. 80, No. 5 (April, 1971), pp. 1035-1069.

the faculty roster of a college, or the donor list of a charity. In these cases, data furnished for one purpose are being used for another, and even though the original source may not have contained more than the name and address, the mere fact of being on the list may reveal something about one's private life.

More serious still are lists derived from actual administrative data systems. There is the strong probability that the original source contained data that might well be intensely personal and that names will be selected for mailing lists on the basis of such data. The data files for driver licenses, for instance, usually contain medical information on disabilities. The administrative files of schools contain grades and other personal items. Any use of files such as these for any but the original intention carries a clear danger of exploitation of truly private personal information.

The Committee staff studied the structure and practices of the mailing-list industry to gauge the threats to personal privacy that could arise from that source, as well as to examine the applicability of the safeguard requirements to the industry. The report of the study is presented in Appendix H; an abstract of its conclusions, which we fully endorse, is given here:

An underlying function of the Advisory Committee's recommended safeguards is to provide effective feedback mechanisms that will help to make automated personal data systems more responsive to the interests of individuals. Systems maintained by most government agencies, and by many private organizations, do not provide for tight links between individuals and the system operators. The direct-mail industry, however, is largely organized around the idea of public feedback; the trade press concentrates almost obsessively on methods for maximizing response and minimizing complaints.

Because most mailings draw a response from only 3 or 4 percent of the addressees, a small change in the response rate can have relatively large economic implications for the mailer. The same is true for the compilers and brokers of mailing lists, because the price a list commands in the rental market depends not so much on its demographic sophistication as on its accuracy and freshness. Lists are cleaned by adding a special imprint to the mailing which gives the Postal Service authority to correct and return (at first-class rates) all undeliverable pieces. Since it costs about four times as much to discover and correct a "nixie" as it does to make a clean mailing in the first place, there is a powerful economic incentive to concentrate lists on known buyers at addresses of known accuracy.

Another feedback mechanism operates on the industry as a whole. Direct-mail advertising is strongly dependent for survival on the official good

will of a large number of agencies of the government; opposition from the Postal Service, from motor vehicle registrars, or from the Census Bureau, to name a few examples, would seriously hamper the industry on its present scale. It seems likely that a scandal involving public records, or the development of a public allergy to direct-mail advertising, would lead to government moves to put constraints on the industry.

Constructive publicity toward emphasizing the rights of the individual relative to direct-mail advertising, especially the methods the industry has adopted for getting off and getting on the larger lists, would go far in strengthening these feedback mechanisms that already operate. In particular, the Direct Mail Advertising Association's Mail Preference Service deserves wider attention.

If feedback mechanisms stronger than those provided by the economics of the industry should become desirable, there would be formidable practical difficulties in applying the Committee's safeguards to the freewheeling small operators of the direct-mail industry. The most directly applicable of the Committee's safeguards is the requirement for the informed consent of the data subject to be obtained before any collateral use may be made of data from an administrative personal data system. To accomplish this, forms that are used by the system in transactions with individuals (applications, for example) and that are vulnerable to mailing-list uses, could be printed with a block in which the individual—by his deliberate action—could indicate whether or not his name and address could be sold or otherwise transferred to another data system for mailing-list use. Of course, this could not prevent his name and address from being copied by hand out of a public record system, but the cost of such handcopying would sharply curtail much commercial use.

In view of the controls already at work in the direct-mail advertising industry, this limited application of the Committee's safeguards seems sufficient. It would provide protection to individuals from having their names unexpectedly appear on mailing lists without their consent. We doubt the utility and feasibility of trying to make the rest of the Committee's proposed safeguard requirements apply to the mailing list as such, as a form of administrative automated personal data system, or to organizations that deal only in mailing lists. If the control of mailing lists is to be undertaken by law, it should be done by legislation that is directed specifically to that purpose.

If the foregoing analysis of the situation underestimates the felt need for greater mailbox privacy, it would be feasible to undertake specific legislative action against the direct-mail advertising industry to provide greater protections, as the regulation of information practices in the consumer-reporting industry amply demonstrates.

A Note on Intelligence Records

In developing safeguard requirements, we have divided personal-data record-keeping systems into two broad categories, (i) administrative systems, and (ii) systems maintained exclusively for statistical reporting and research. The distinction between the two is in their purpose vis-a-vis individuals. Administrative systems are intended to be used to affect individuals as individuals; statistical reporting and research systems are not. According to this classification, intelligence records are properly considered administrative records.

A chief characteristic of intelligence records is that they are compiled for purposes that presuppose the possibility of taking adverse action against an individual. Their focus is on providing a basis for protecting the data-gathering organization, or other organizations that it serves, against the individual. There are many examples of intelligence-type personal-data record-keeping systems. From a historical standpoint, the original and classical intelligence records were those compiled and maintained about individuals who were viewed as possible enemies of the state. The most obvious and perhaps most common ones today are those compiled by the criminal intelligence systems of Federal, State, and local law enforcement agencies about individuals suspected of being engaged in criminal activities, of being threats to public safety or national security, or of being suitable objects of surveillance and investigation for less clearly definable reasons. There are, however, many other examples of intelligence-type records, including investigative records of credit-reporting agencies, private detective agencies, industrial security organizations, and so on. It is hard to know how many types of intelligence data systems exist because their function leads as a rule to careful concealment.

In framing our proposed safeguard requirements for administrative personal data systems, we did not focus on intelligence records as such. We realize that if *all* of the safeguard requirements were applied to *all* types of intelligence records, the utility of many intelligence-type records for the purposes they are designed to serve might be greatly weakened. In some instances this would clearly not be a desirable outcome from the standpoint of important societal interests, such as the apprehension and prosecution of individuals

engaged in organized crime. It does not follow, however, that there is no need for safeguards for personal-data intelligence record-keeping systems. The risk of abuse of intelligence records is too great to permit their use without *some* safeguards to protect the personal privacy and due process interests of individuals.

The mere gathering of intelligence data can be a serious threat to personal privacy and should be carried out with strict respect for the Constitutional rights of individuals. Once criminal intelligence data have been compiled, their use in connection with law enforcement prosecutions is safeguarded by all the Constitutional requirements of due process and by laws that establish limitations on the exercise of the police power, including civil and criminal remedies and penalties that may be imposed to enforce such limitations. We have not attempted to assess whether protections now afforded individuals from abuses of intelligence records as used in criminal law enforcement should be strengthened.

We are concerned, however, about the use of criminal intelligence data, and intelligence records maintained by organizations other than law enforcement agencies, for many purposes that involve determinations about the qualifications, character, opportunities, or benefits of individuals to which the protective requirements of due process may not apply or for which they may not be fully effective. Such determinations include suitability for employment, especially in public service or in positions of critical fiduciary responsibility; clearance for access to classified national security information held by the Federal government and its contractors; and eligibility for various public benefits, permits, and licenses.

Enactment of the proposed Code of Fair Information Practice for administrative personal data systems will afford an excellent opportunity to determine precisely what protections for individuals should be applied to intelligence record-keeping systems. Any exception from a safeguard requirement that is proposed for any type of intelligence system must be specifically sanctioned by statute and then only if granting the exception would serve a societal interest that is clearly paramount to the interest served by having the requirement imposed.

The process of considering exceptions for intelligence systems will entail a careful review of existing policies, laws, and practices governing the creation, maintenance, and use of intelligence records about individuals. The need for such a review has seldom seemed more urgent in the history of our Nation.

... in an information-rich world, the wealth of information means a dearth of something else: a scarcity of whatever it is that information consumes. What information consumes is rather obvious: it consumes the attention of its recipients. Hence a wealth of information creates a poverty of attention and a need to allocate that attention efficiently among the overabundance of information sources that might consume it.

Herbert Simon, "Designing
Organizations for an
Information-Rich World."*

"He had been kicked in the head when young and believed everything he read in the Sunday Papers."

George Ade, *Fables in Slang:
The Slim Girl*

*In Martin Greenberger (Ed.), *Computers, Communication, and the Public Interest* (Baltimore, Md.: The Johns Hopkins Press), 1971, pp. 40-41.

V

Statistical-Reporting and Research Uses of Administrative Data Systems

Many automated personal data systems established primarily for administrative purposes are also used for statistical reporting and research. Since one advantage of computerizing administrative records is the capability thereby acquired for high-speed data retrieval and manipulation, a growing number of administrative data systems will be put to such additional uses. The safeguard recommendations in this chapter take account of that expectation.

Dimensions of the Problem

A modern organization, as a rule, maintains elaborate records about the money it spends, the people it serves, the quantities of goods and services it dispenses, and the number, qualifications, and salaries of the people who work for it. It does so, in part, because it must account for its activities to investors or taxpayers, and to other organizations that monitor and regulate its behavior.

An organization also needs to plan for the future. A firm selling to the public is interested in knowing what the public wants, or can be persuaded to want. A school needs to know about the financial and intellectual capabilities of students coming to it for learning. A government agency tries to forecast demand for the services it provides or supports.

These incentives to develop indicators of institutional performance make it difficult to control the quantity and variety of personal data stored in administrative record-keeping systems, and the statistical-reporting and research uses that are made of such data. The personal data that organizations collect for administrative purposes should be limited, ideally, to data that are demonstrably relevant to decision making about individuals. A substantial amount of personal data, however, appear to be collected because at some point someone thought they might be "useful to have," and found they could be easily and cheaply obtained on an application form, or some other record of an administrative transaction.

For example, college students applying for government-guaranteed loans in one State have been required to provide the State guarantee agency with data on matters that had no direct relation to its individual entitlement decisions. These data, "for our statistical interest" as their intended use was described to the Committee, included race, marital status, sex, adjusted family income, and student-reported "average grades received for last term of full-time post-high school study." These data have been used to produce statistical reports for internal agency use, for informal discussions with State legislators, and to "run a profile once yearly on . . . schools and . . . lenders to see if there is any odd pattern . . . occurring." On one occasion data in the system also have been used in a study conducted by an outside researcher. For making entitlement decisions, however, the data being collected in excess of those required by law were described to us as not very helpful to the program, and at least two data elements—sex and student-reported grades—were said to be absolutely valueless.¹

¹ A representative of the State agency told the Committee that the agency would not compel a student applicant to provide this information "because we have come to find it is totally worthless . . . [A]t one time we thought it would be a viable way of sampling the type of student we would assist. We determined it is not much use . . . [but w]e have not taken it out."

The student loan case is but one illustration. The presentations of system managers and users yielded others. We found that decisions to collect personal data are being made without careful consideration of whether they will in fact serve the purposes for which they are supposedly being collected. As a result, substantial sums may be spent on comprehensive data collections for purposes that could often be much better served by other approaches, such as collecting statistical-reporting and research data only from a small sample of an organization's clients or beneficiaries. Most disturbing of all, we found that personal data in excess of those clearly needed for making decisions about individuals are sometimes collected in a way that makes them seem prerequisite to the granting of rights, benefits, or opportunities.

Mandatory or Voluntary Data Collection?

Poorly conceived data collection can result in various kinds of injury to individuals. As observed earlier, any file of personal data is a potential source of harm to individuals when it is used outside its appropriate context, and much of the personal data in administrative files either is a public record or is vulnerable to legal process.

There is also reason to believe that failure to separate information collected for statistical-reporting or research from data used in entitlement decisions may cause such decisions to be made unfairly. "Race" and "sex" are no longer asked on many application forms because of their acknowledged influence on some types of decision making about individuals. There are circumstances in which other kinds of data may have similarly unwarranted effects.² Moreover, collecting more information than is needed for day-to-day administrative decisions may discourage people from taking advantage of the services an organization offers. As one witness told the Committee:

² For a cogent analysis of the effects of "contextual" information on clinical disability determinations, see Saad L. Nagi, *Disability and Rehabilitation* (Columbus, Ohio: Ohio State University Press), 1969, especially Chapters 2 and 9. Discussion of this problem will also be found in Stanton Wheeler (Ed.), *On Record: Files and Dossiers in American Life* (New York: Russell Sage Foundation), 1969.

.... our experience indicates that rigid adherence to proper data collection often "turns off" many clients, even when the interviewer is ingenious at gathering it. Also counselors often openly resent [having to ask] questions which actually may jeopardize their relationship with a client.

Perhaps most important of all is the intrusive effect of unrestrained data collection on self-esteem. Occasionally one hears that a wealthy citizen has hired a chauffeur and limousine to avoid disclosing his Social Security number, or some other item of information, to a State Department of Motor Vehicles. One is tempted to dismiss such protests as the trivial antics of rich eccentrics; yet they indicate the high cost of trying to escape personal inquiries of organizations that monopolize the distribution of certain privileges and benefits. The plight of the welfare beneficiary is especially extreme in this respect, but with all the forms that everyone of us is constantly filling out, it would probably be hard to find a single individual who has not had one occasion at least to wonder, "Why do they want to know that?" and "What will happen if I refuse to tell them?"

Collecting statistical-reporting and research data in conjunction with the administration of service and payment programs is not intrinsically undesirable. However, such supplementary data gathering should be carefully designed and managed, and should be performed only with the voluntary, informed cooperation of individual respondents. Otherwise only personal data directly and demonstrably germane to a decision about any given individual should be collected.

Separate collection of data for statistical reporting and research could have several practical advantages. First, by increasing the cost of supplementary data gathering, it discourages the collection of useless items. Second, it might reduce the amount of data that must be specially protected because it is identifiable. Although personal data maintained *exclusively* for statistical reporting and research often need broader and stronger protection than they are afforded,³ differentiating sharply among the purposes and uses of

³ The special problems of data maintained *exclusively* for statistical reporting and research are discussed in Chapter VI.

data files should encourage public confidence in organizational record-keeping practices and ease the access control burden that now weighs heavily on some system managers.

Third, separate collection of personal data for statistical reporting and research could help to make the collection process more reliable. We learned of instances in which an ambitious information system's appetite for data has induced careless statistical reporting. This problem appears to be especially prevalent where an information system has been established to help coordinate the activities of a number of small, loosely knit organizations. Such carelessness can frustrate the management objectives of a system by diluting the quality of data furnished to it in ways that may not be recognized or, if recognized, may be very difficult to control.⁴

Assuring Sound Secondary Uses of Administrative Data Systems

Administrative record-keeping operations can and do constitute rich sources of statistical-reporting and research data useful for many purposes. For example, the Federal government uses Internal Revenue Service records as a source of data for the quinquennial Census of Business and Manufacturers; hospital records are used to develop research data banks on particular diseases or disabilities; school and college records are used to study the relationship between academic performance and subsequent career achievement. Unfortunately, however, the mere existence of an administrative data base can create a strong temptation to use it for statistical reporting and research without sufficient attention to the appropriateness of doing so.

⁴As one representative of a small group of agencies observed in his testimony before the Committee:

Client- (rather than management-) oriented agencies are philosophically committed to research *only secondarily*, as a tool for delivering more effective services. Therefore, they often must be dragged kicking and screaming into the data collection business. This is totally apart from their finances or their training . . . Where services are . . . interfered with, data collection goes out the window. Measurement error can then be quite high.

Three conditions that encourage sound use of data systems for statistical reporting and research are often absent from the environment in which administrative systems are designed and operated. They are:

- knowledge of the social processes by which data come to be collected;
- management of data collection and analysis by individuals with strong statistical and research competence; and
- independent expert scrutiny of analytic methods and results.

Knowledge of Data Collection Processes. Detailed understanding of how and why data come to be collected is often difficult, if not impossible, to achieve. For example, not everyone who is eligible for public assistance applies for it, and the amount and kind of information collected from each applicant may vary in subtle ways.⁵ Hence, if data from administrative systems are used for statistical reporting and research, the results must take account of systematic bias resulting from incompleteness in the data base. Measuring such bias can be expensive and time-consuming, and corrections for it can be even harder to make. Highly trained people are needed to conduct careful studies of the processes by which data in a system are being generated. Because of their expense and difficulty, however, and also because they can bring to light inadequacies in the overall performance of an organization, such studies tend not to be done.

Statistical and Research Competence. Because most administrative systems are committed to day-to-day record-keeping operations, they are seldom managed or staffed by persons with strong statistical and research competence. It is true that the statistical agencies of a few large government agencies—notably the Social Security Administration and the Internal Revenue Service—have substantially influenced the statistical uses made of their principal data

These variations may result from practices rooted in a bureaucratic subculture of which the record-keeping operation is but one—albeit important—part. See, for example, the discussions of how juvenile court, welfare, credit, and elementary school records are generated, in Wheeler, *op. cit.*, Chapters 2, 5, 11, and 12.

sources, which are mainly administrative records. Similar examples can be found at other levels of government and among private organizations, but there are also numerous instances in which such statistical and research competence is brought to bear only through informal or sporadic consulting arrangements, if at all.

Independent Scrutiny. Because administrative data systems are not created expressly for statistical reporting and research, they also tend to lack the strong ties to external groups of data users, and to the formal systems of professional peer review that characterize general purpose statistical-reporting and research operations. This isolation from independent expert scrutiny, coupled with the management orientation of administrative data systems, weakens the incentive to maintain high standards in the secondary statistical-reporting and research uses that are made of them.

Neglect of these three conditions is particularly dangerous in a governmental setting. In business, the quality of statistical reporting and research may be measured by the usefulness of such work to the planning and marketing functions that maintain a firm's competitive position. In government, however, feedback from the marketplace is attenuated. Save for the occasional newsworthy statistical report, the ancillary uses of administrative data systems may be ignored by outside professionals and invisible to the general public and its elected representatives.

In the Federal Government, formal arrangements for implementing the Federal Reports Act are supposed to serve as a check on the uses made of administrative record-keeping systems for statistical reporting and research. However, at other levels of government, the low visibility of such uses, coupled with the uneven impact of public information laws, can create an open invitation to misguided use of statistical reports and research findings based on administrative data.

We learned, for example, that one agency of a State government recently attempted to compare earnings declarations made by some public assistance beneficiaries to county welfare offices, with earnings of those same beneficiaries reported by their employers to a second State agency. This complex comparison of data derived from two quite different administrative record-keeping systems was

undertaken mainly to verify the beneficiaries' eligibility for public assistance payments on a case-by-case basis, but it also resulted in a statistical report "showing" that a substantial percentage of the State's public assistance beneficiaries were engaged in "apparent fraud." The design of the comparison, and thus the resulting data, supported no such conclusion. Few people are aware of its technical failings, however, and it seems unlikely that many more will discover them, since appropriately documented data from the study have not been made available outside the sponsoring State agencies.

Recommendations

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.⁶

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.⁷

⁶ Recall in this regard safeguard requirement III (1), recommended in Chapter IV (p. 59, above) for all administrative automated personal data systems; viz., that *an individual asked to supply data for a system be informed clearly whether he is legally required or free to refuse to provide the data requested*. That safeguard, when applied, will effectively eliminate *de facto* coercion of data subjects into providing more information than is needed for making administrative decisions.

⁷ Separating the two types of data in this way would make it easier to apply the protection against compulsory disclosure recommended in Chapter VI (pp. 102-103, below).

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.

It would be difficult to apply each of these principles uniformly to all administrative automated personal data systems. For this reason, we have not translated them into safeguard requirements to be enacted as part of a code of fair information practice. Adherence to their spirit, however, is warranted by the growing significance of statistical-reporting and research uses of administrative personal data systems—both for individual data subjects and for the institutions maintaining such systems.

In addition, there are certain safeguards that can be feasibly applied to all administrative automated 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 (Chapter IV, pp. 53-57), 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 administrative 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 (Chapter IV, p. 58), 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.

The purpose of general requirements *C. (1)* and *C. (2)* is to assure that when statistical reports or research findings based on personal data from administrative systems are used to affect social policy, the data will be available, in an appropriate form, for independent analysis. To comply with this requirement, an organization will have to plan carefully all publicly disseminated statistical-reporting and research uses of personal data in the administrative systems it maintains.

The public notice for an administrative personal data system will specify any statistical-reporting and research uses to be made of data in the system (requirement *II. (7)*, p. 58) The additional information required by requirement *(8a)* will make it easier to obtain access to data for independent analysis.

Sweet Analytics, 'tis thou has ravished me!

Marlowe, *Faustus*, I, 34

VI

Special Problems of Statistical-Reporting and Research Systems

When the United States was at war with Japan in 1942, the War Department asked the Census Bureau for the names and addresses of all Japanese-Americans who were living on the West Coast at the time of the 1940 Census. Persons of Japanese descent were being rounded up and transported inland for fear that some of them might prove disloyal in the event of a Japanese attack. Because of Title 13 of the U. S. Code, however, which prohibits disclosure of census data furnished by individuals, the Census Bureau could, and did, refuse to give out the names and addresses.

In 1969, the Mercer County (N.J.) Prosecutor's Office subpoenaed the payment histories of 14 families participating in an income-maintenance experiment being conducted by a private contract research organization in Princeton. The prosecutor suspected that the families were defrauding the county welfare department by not reporting their monthly income from the experiment. The contractor found that it had no legal basis for resisting the subpoenas, even though its federally funded subcontract explicitly provided that "individual personal and financial information pertaining to all

individuals and families who participate as respondents in this study shall remain strictly confidential."¹

The difference between these two cases is clear and fundamental: In the Census case, the data were protected by a statute² from disclosure in individually identifiable form; in the New Jersey case they were not.³ This chapter examines some of the problems posed by legally unprotected statistical-reporting and research files that contain data about identifiable individuals. It focuses on the need to protect individual data subjects from injury through disclosure of data about them, on one hand, and, on the other, the need to make files of personal data more accessible to persons who can make constructive use of the data they contain.

Background Observations

When we began our examination of automated record-keeping operations, we expected that we could leave out entirely data

¹David N. Kershaw and Joseph C. Small, "Data Confidentiality and Privacy: Lessons from the New Jersey Negative Income Tax Experiment," *Public Policy*, Vol. XX, No. 2 (Spring 1972), p. 261. The Mercer County dispute stemmed from a change in the State public assistance law which made more participants in the experiment eligible for welfare than had been the case when the experiment began. The 1969 investigation was terminated when the contractor agreed to reimburse the county welfare agency for any overpayments that came to light. Two years later, however, the experiment was subjected to a four-month grand jury investigation of charges that the contractor had "instructed low-income families taking part in the experiment not to report income subsidies to city and county welfare authorities . . ." *Ibid.*, p. 268. During this same period, access to the contractor's files was also sought by the General Accounting Office and the U. S. Senate Finance Committee.

²The current version of this protection provides that:

Neither the Secretary, nor any other officer or employee of the Department of Commerce or bureau or agency thereof, may . . . (1) use the information furnished under the provisions of this title for any purpose other than the statistical purposes for which it is supplied; or (2) make any publication whereby the data furnished by any particular establishment or individual under this title can be identified; or (3) permit anyone other than the sworn officers and employees of the Department or bureau or agency thereof to examine the individual reports. . . . 13 U.S.C. 9(a).

³The New Jersey case is not unique. At least two other incidents of a similar nature have been reported. See John Walsh, "Anti-poverty R&D: Chicago Debacle Suggests Pitfalls Facing OEO," *Science*, 165, 19 September 1969, pp. 1243-1245; and "Appeals Court Orders MD to Reveal Patients' Photos," *Psychiatric News*, VII:2, November 15, 1972, p. 1. The latter describes a pending court case involving the New York City Methadone Maintenance Treatment Program.

systems maintained *exclusively* for statistical reporting or research. We were mindful that in the mid-1960's a series of proposals⁴ to establish a national statistical data center had alerted the public to some of the dangers inherent in computer-based record-keeping operations. We also knew that the Freedom of Information Act contains no clear statement of Congressional intent with respect to the disclosure of individually identifiable data maintained for statistical reporting and research. We had assumed, however, that statistical-reporting and research data systems, by and large, would not contain data in personally identifiable form, and that if they did, the anonymity of individual data subjects would be protected by specific statutory safeguards. We were not prepared for the discovery that in many instances files used exclusively for statistical reporting and research do contain personally identifiable data, and that the data are often totally vulnerable to disclosure through legal process. This holds for data in Federal agency files as well as for data in the possession of State agencies and private research organizations.

Changes in social policy, which computer technology has to some extent facilitated, are in large part responsible for the existence of unprotected statistical-reporting and research files. Since the late 1950's, the Federal Government has been distributing increasingly large sums of money to the States on the basis of formulas that take account of special population characteristics. The recipient State governments, in turn, have been redistributing this money among their own political subdivisions, using grant-in-aid formulas that tend to generate new requirements for statistical data about people at nearly every level of government. Often coupled with these grants, moreover, have been planning requirements demanding highly detailed information about the populations of small geographic areas.

Program evaluation requirements, first levied on grant-in-aid recipients by Federal agencies and later explicitly written into some

⁴*Report of the Committee on the Preservation and Use of Economic Data to the Social Science Research Council*, April 1965, reprinted as Appendix I in *The Computer and Invasion of Privacy*, Hearings before a Subcommittee of the Committee on Government Operations, U. S. House of Representatives, 89th Congress, 2d Session, July 26, 27, 28, 1966; *Statistical Evaluation Report No. 6—Review of Proposal for a National Data Center*, prepared by Edgar S. Dunn, Jr., also reprinted in *The Computer and Invasion of Privacy as Appendix 2*; and *Report of the Task Force on the Storage of and Access to Government Statistics* (Washington, D.C.: Bureau of the Budget), October 1966.

of the agencies' authorizing legislation, have been a further stimulus to the proliferation of statistical-reporting and research files containing data about people. From their initial emphasis on simple input accounting (how much was spent, by whom, for what purpose, on how many people, with which characteristics), evaluation studies have rapidly come to focus on measuring program effects.⁵ Because effects measurement usually requires before-and-after data on program participants, it has become necessary to preserve individual identities in evaluation research files. Interest in the specific events and processes that may account for changes in participant behavior over time has also grown along with interest in output measurement. Many of the factors that account for a participant's behavior are so subtle that they can only be isolated if records of people's movements and experiences are kept over an extended period.

A third factor that has enlarged the number of data files containing information about identifiable individuals is the broad support given to fundamental research in the social and biomedical sciences. In fact, files for research in these two areas may be the most numerous of all, and they exist in a variety of settings. Many such files are coming into the possession of government agencies as a consequence of contract arrangements that make agencies the proprietors of data generated in government-supported research and demonstration projects. Not all of these files contain information that identifies individual data subjects, but of those that do, the ones dealing with controversial social and political issues are particularly vulnerable to misuse in the absence of specific statutory safeguards.

The Need to Protect Data Subjects From Injury

Even at the Federal level there are few statutes that protect personal data in statistical-reporting and research files from unintended administrative or investigative uses. The Census Act, the

⁵ There is today a substantial evaluation research literature to which the interested reader can refer for a fuller account of how this new government-supported activity has developed. See, for example, Edward A. Suchman, *Evaluative Research* (New York: Russell Sage Foundation), 1967; Francis G. Caro, *Readings in Evaluation Research* (New York: Russell Sage Foundation, 1971); and Peter H. Rossi and Walter Williams (Eds.), *Evaluating Social Programs: Theory, Practice, and Politics* (New York and London: Seminar Press), 1972.

Public Health Service Act, and the Social Security Act are notable exceptions. Otherwise there is little to prevent anyone with enough time, money, and perseverance (to say nothing of someone who can issue or obtain a subpoena) from gaining access to a wealth of information about identifiable participants in surveys and experiments. This should not, and need not, be the case.

Social scientists and others whose research involves human subjects are vocal about the importance of being able to assure individuals that information they provide for statistical reporting and research will be held in strictest confidence and used only in ways that will not result in harm to them *as individuals*. Unless people get—and believe—such assurances, they will inevitably become either less willing or less reliable participants in surveys and experiments.⁶ Ideally, data subjects should also be told of the conditions under which they are being asked to provide information, and should be given an opportunity to refuse if they find those conditions unsatisfactory. It is often asserted, for example, that the decennial census (in which response is mandatory) is a feasible undertaking only because the public willingly co-operates, and that the public's cooperation is best obtained by explaining to respondents the uses to which the data will be put.

We believe the principle that no harm must come to an individual as a consequence of participating in a general knowledge-producing activity should be regarded as the essence of "use for statistical or research purposes only." Individual data subjects asked to provide data for statistical reporting and research should also be fully informed, in advance, of the known consequences for them of providing or not providing data. Survey respondents and participants in experiments and demonstration projects are largely dependent on what they are told by interviewers or by explanatory notes on forms. Hence, it is incumbent on the institution conducting or funding a statistical-reporting or research project to find out how vulnerable the data in its files are, and so to inform its data subjects.

Finally, we believe that the best way to assure that individual data subjects will not be harmed is to extend to all personal data generated through statistical-reporting and research activities the

⁶ See Chapter 6, "Privacy and Confidentiality," in *Federal Statistics*, the Report of the President's Commission on Federal Statistics (Washington, D.C.: U.S. Government Printing Office), 1971.

statutory protections that have been given to census data and certain classes of health and economic data collected and used in the public interest.

The Need for Freer Access to Data in Government Files

The obverse of the problem of data confidentiality is the need to make basic data more accessible for reuse or reanalysis by all qualified persons or institutions. Personal data systems for statistical reporting and research are largely in the hands of institutions that wield considerable power in our society. Hence, it is essential that data which help organizations to influence social policy and behavior be readily available for independent analysis.

The ubiquitous computer has increased both the quantity of data potentially available to users and the number of potential users. Unfortunately, however, the data dissemination capability of many funding and collecting institutions has not grown commensurately. Among the general purpose statistical operations of the Federal government, the Census Bureau has led the way in making data from standard statistical series easily available to users in a form that protects the anonymity of respondents. Other agencies, notably the National Center for Health Statistics, have followed suit.⁷ The Department of Health, Education and Welfare is currently preparing a guidebook of its "public use" data files.⁸

Laudable as these efforts are, it should be emphasized that they are being made, for the most part, by agencies or offices within agencies whose primary mission is statistical reporting and research. They do not address the problem of access to the statistical-reporting and research files that operating agencies develop in the course of evaluating programs or in adding to the general knowledge of program administrators. It is true, as noted earlier, that anyone with enough money, time, and perseverance can probably gain access to substantial amounts of data not generally available for public use. Yet the individual researcher, or the independent critical

⁷National Center for Health Statistics, *Standardized Micro-Data Transcripts* (Rockville, Md.: National Center for Health Statistics), December 1972.

⁸*Guidebook to the U.S. Department of Health, Education, and Welfare Computer Data Files*, 1973 (forthcoming).

expert, however perseverant, may not even know that important data exist, much less where to find them. If he does find them, and if he can afford to have them put in usable form, the documentation may not be sufficient to permit reconstruction of the conditions and suppositions under which the data were collected. An agency holding data collected under a pledge of confidentiality may not be willing to go to the trouble (or may itself not be able to afford the cost) of expunging elements that would serve to identify individual data subjects in order to make the data available.

In principle, there need be no conflict between informing the public about how the government conducts its business and protecting individual data subjects from harm. If data cannot be made available for reuse or reanalysis without disclosing the identity of data subjects, special precautions may have to be taken before making basic data accessible to qualified persons outside the collecting organization, but such precautions can be taken. For example, each data subject could be asked at the time of the initial data collection if he would consent to participate in a follow-up study, on the understanding that consent would be sought anew each time a further follow-up study is undertaken. Although such arrangements may add to the expense and difficulty of some data collections, a public institution that uses scientific approaches and methods has a duty to make the work it sponsors or supports available for critical appraisal.

Making fully documented data available for reuse and reanalysis by persons competent to assess the interpretations that have been made of them can bring two benefits. First, the knowledge that other investigators will have an early opportunity to challenge its conclusions should tend to heighten the quality of the original collection and analysis, and second, advances in the sciences may produce more powerful techniques of analysis that could make it possible to glean additional information from data in the course of re-examining them.

Recommendations for Statistical-Reporting and Research Systems

In Chapter IV, we have recommended enactment of legislation establishing a code of fair information practice for all automated personal data systems. All the features of that code would apply to systems used exclusively for statistical reporting and research. The

safeguard requirements to be included in the code for such systems are set forth below. They are designed to help protect the individual citizen against unintended or unforeseen uses of information he provides exclusively for statistical reporting and research, and to help assure that the uses organizations make of statistical-reporting and research data are subjected to independent expert review and open public discussion. Pending the enactment of a code of fair information practice as outlined in Chapter IV, we recommend that all Federal agencies (i) apply the safeguard requirements, by administrative action, to all Federal statistical-reporting and research systems, and (ii) assure, through formal rule making, that the safeguard requirements are applied to all systems within reach of the Federal government's authority. 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.

In addition, we recommend that all personal data in systems used exclusively for statistical reporting and research be protected by statute from compulsory disclosure in identifiable form. The safeguard requirements recommended below are premised on the enactment of legislation granting such protection. There is no requirement, for example, guaranteeing data subjects access to the contents of records maintained about them. Theoretically, no such requirement is needed, since statistical-reporting and research data systems are not intended to be used to affect individuals directly; granting individuals access to records that can have no direct consequences for them *as individuals* would interfere with a system's operations to no useful end. In practice, however, the vulnerability of data in many statistical-reporting and research systems to compulsory disclosure in identifiable form means that for individual data subjects to be adequately protected from unforeseen disclosures, those data must be afforded immunity from disclosure through compulsory legal process.

The safeguard requirements for statistical-reporting and research systems are modeled closely on the safeguard requirements for administrative systems in Chapter IV. Hence explanatory notes are provided only in those cases where a requirement has been modified to fit the special characteristics of statistical-reporting and research

systems. Where no notes appear following a requirement, the reader should refer to the notes on the corresponding safeguard in Chapter IV.

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 (in Chapter IV).

All other safeguard requirements for statistical-reporting and research systems have been formulated to apply only to *automated* systems, although they would wisely be applied to all statistical-reporting and research systems, whether automated or manual. If this is not done, however, it is necessary to assure that individuals about whom an organization maintains records of personal data, which are not part of an automated system, will be protected in the event of transfers of such data to automated systems. Requirement I.A. is intended to provide such protection for individuals by requiring that transfers of data about them to automated systems not subject to safeguard requirements be made only with their informed consent.

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;

The obligation to identify a person responsible for the system is intended to provide a focal point for assuring compliance with the safeguard requirements and to guarantee that there will be someone with authority to whom individuals, groups, or organizations can go if other methods of dealing with the system are unsatisfactory. Systems that involve more than one organization may present special problems in this respect, and must be carefully designed to assure that a person is not shuffled from one organization to another when he seeks to assert any right under these 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;

Requirement (5) has basically the same implications for statistical-reporting and research systems that it has for administrative systems (Chapter IV, p. 56). However, applied to statistical-reporting and research systems along with requirement III (2) (p. 101, below), requirement (5) will also prevent

an organization or a researcher from transferring data in identifiable form to another organization or researcher who could not fully guarantee that the transfer would result in no uses of the data not reasonably anticipated by the data subjects.

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

This requirement should be understood to mean that data whose use helps an organization to influence social policy and behavior must be readily available. In cases where independent analysis could not be performed without knowing the identity of each data subject, a system would be considered fully "capable" if, for example, it had obtained the consent of each data subject to participate in a follow-on study, or had a policy of seeking the consent of data subjects on behalf of persons wanting to perform such 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:

- (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.

This requirement has two primary objectives: (1) to assure that there will be no automated personal data system whose very existence is kept secret from the public; and (2) to assure that uses of systems by organizations to help them influence social policy or behavior are not immune from independent expert scrutiny. Instances will no doubt arise in which announcement of a research project prior to undertaking it could seriously hamper part of the study. In other instances, the scale of a project might be so small, and its influence on social policy so remote, that strict compliance with the public notice requirement will seem unduly burdensome. For such cases some mechanism will have to be devised for granting exemptions from the public notice requirement. Because of the diversity of statistical-reporting and research activities that organizations conduct, sponsor, or support, we have not tried to specify criteria for granting exemptions or to prescribe any particular mechanism for dealing with requests for exemptions on a case-by-case basis. We do feel, however, that the people who want to do research that might qualify for an exemption should not be asked to bear the full burden of deciding whether an exemption is appropriate.

The matter of exemptions from the public notice requirement is one to which careful attention will have to be addressed when the safeguard requirements are being applied by administrative action, and eventually in connection with the enactment of legislation establishing the code of fair information practice for statistical-reporting and research systems.

We have also refrained from specifying a uniform mechanism for giving notice. For Federal agencies, we would expect formal notice in the *Federal Register*, but a catalog of data files published annually would also suffice. We would expect State and local governments to use whatever comparable mechanisms are available to them. Other systems may find that notices given through professional journals or mailings would be appropriate. Whatever methods are chosen, an organization must have copies of its notices readily available to anyone requesting 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;

As indicated in Chapter IV (p. 59, above), one purpose of this requirement is to discourage coercive collection of personal data that are to be used exclusively for statistical reporting and research. However, the requirement that an individual be informed of the consequences of providing, or not providing, data for a system is also intended to assure that no pledge to hold data in confidence will be given by a data-collecting organization without apprising each data subject of the legal limitations, if any, of such a pledge.

- (2)⁹ 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;

⁹This requirement corresponds to requirement III(3) in Chapter IV.

(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.

The intent of this requirement is similar to that of requirement III (5), as explained in Chapter IV (p. 63, above). Because there is no safeguard requirement for statistical-reporting and research systems giving an individual the right of access to data about himself (as provided in requirement III (2) for administrative systems), this requirement gives an individual that right in the event of a compulsory process demand. The need for this requirement would be obviated by enactment of legislation providing effective protection against compulsory disclosure of identifiable personal data maintained in statistical-reporting and research systems. However, until such legislation is enacted, or if, when enacted, the legislation leaves an organization maintaining such a system any discretion whatsoever to waive the protection against compulsory disclosure, this safeguard should be the minimum protection afforded individual data subjects.

Statutory Protection Against Compulsory Disclosure

A primary goal of safeguard requirements for statistical-reporting and research systems must be to protect individual data subjects from harm. That goal will be frustrated if, after having been assured that the data he provides for a system will be seen only by persons formally involved in the statistical-reporting or research project, a data subject finds that the data have been disclosed in identifiable form in response to a subpoena.

Statistical-reporting or research data that can be traced to identifiable individuals should not be subject to compulsory disclosure through legal process. **In our view, there must be new Federal legislation protecting against such disclosure, and it 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.¹⁰
- 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"¹¹ should be considered to fulfill the obligation not 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.
- The Federal law should be controlling; no State statute should interfere with the protection it provides. (The need also exists for State legislation to protect statistical-reporting and research data that cannot be reached by Federal legislation.)
- 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.

¹⁰ See Note 7, Chapter V, p. 85.

¹¹ This is a risk that arises when a population is so narrowly defined that tabulations are apt to produce cells small enough to permit the identification of individual data subjects, or when a person using a statistical file has access to information which, if added to data in the statistical file, makes it possible to identify individual data subjects. See I. P. Fellegi, "On the Question of Statistical Confidentiality," *Journal of the American Statistical Association*, 67:337 (March 1972), pp. 7-18.

These are essential conditions for protecting statistical-reporting and research data from compulsory disclosure in identifiable form. Legislation incorporating the features indicated would not prevent the disclosure of basic records from a statistical-reporting or research system so long as data in the records could not be traced to specific individuals.

We offer no specific guidance on the form of the statutory protection. However, existing Federal confidentiality statutes contain some relevant examples. These range from absolute prohibitions against disclosure to authority for an administrative official to make disclosure regulations. Among the specific methods are the following:

Absolute Prohibition of Disclosure. Two existing statutes provide stringent protections for personal data held by Federal agencies.

(a) Data collected by the Bureau of the Census may not be revealed to anyone outside of the Bureau in a form in which an individual respondent is identifiable. There is no discretion for any Bureau official with respect to disclosure. There are criminal penalties for disclosure. The prohibition against disclosure serves to defeat legal process. If a respondent retains a copy of a report made to the Bureau, the copy, like the original, is immune from process. 13 U.S.C. 9,214.

(b) Data collected under the National Health Survey may not be used "for any purpose other than the statistical purpose for which it was supplied except pursuant to regulations of the Secretary [of Health, Education, and Welfare]; nor may any such information be published if the particular establishment or person supplying it is identifiable except with the consent of such establishment or person." Sec. 305(a) of the Public Health Service Act, 42 U.S.C. 242c. Here again, the holders of the records are given no discretion to reveal information or withhold it; only the establishment or the person who supplied the information has that discretion. Criminal penalties for disclosure derive from a general statute on disclosure of confidential information. 18 U.S.C. 1905.

Absolute Protection Against Compulsory Disclosure. A second pattern of data protection is provided by statutes that authorize a Federal official to authorize others to protect the privacy of individuals who are the subject of research by withholding from all persons not connected with the research the names and other iden-

tifying characteristics of such individuals. Such authority is vested in the Secretary of Health, Education, and Welfare by Section 303(a) of the Public Health Service Act, 42 U.S.C. 242a, with respect to drug research, and also by Section 333 of the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970, 42 U.S.C. 4582, with respect to alcohol abuse and alcoholism research. Similar authority is given the Attorney General by Section 502(c) of the Comprehensive Drug Abuse Prevention and Control Act of 1970, 21 U.S.C. 872(c), with respect to "research." The latter authority speaks only of "research," but appears in a section of the statute dealing with research related to enforcement of laws concerning drugs.

The authority in each of these instances is explicit as to immunity from process. Those who obtain the authorization "may not be compelled in any Federal, State, or local civil, criminal, administrative, legislative, or other proceeding" to identify the subjects of research. These sections are of wide scope. The authorization may be given to anyone engaged in the specified type of research. Thus, the Secretary or Attorney General can extend it to Federal employees under his control Federal employees in other agencies, grantees, and even to researchers who are not grantees. However, there is no absolute prohibition on disclosure. The Secretary or Attorney General may grant or withhold the authorization. The researcher with the authorization "may not be compelled. . . to identify such individuals," but may choose to identify them pursuant to process or otherwise, subject to whatever other ethical or legal constraints exist. Thus, it is not strictly a privilege, like the lawyer-client privilege, in which the individual who has provided the information controls the action of the professional in responding to process.

Discretion to Disclose Under Specified Conditions. The Drug Abuse Office and Treatment Act of 1972 (P.L. 92-255) provides a third model. Section 408 of that Act, 21 U.S.C. 1175, establishes as confidential, and forbids disclosure of, patient records "which are maintained in connection with the performance of any drug abuse prevention function authorized or assisted under any provision of this Act or any Act amended by this Act." There is a criminal penalty for disclosure. If the patient gives written consent, the record may be disclosed for medical care purposes, or to govern-

mental personnel in order to obtain benefits for the patient. If the patient does not give consent, the record may be disclosed for emergency medical treatment; for research, audit, or evaluation purposes (as long as the patient's identity is not further disclosed); or if authorized by a court order upon application showing good cause. Criminal charges may not be initiated or substantiated on the basis of patient records, and patients may not be investigated on the basis of patient records, except pursuant to disclosure under a court order. The section continues to apply to a patient's records after he ceases to be a patient.

This statute speaks of records "maintained in connection with any drug abuse prevention function," and this seems to include records kept solely for research, but the term "patient" is used repeatedly. The Act's legislative history shows that confidentiality was provided so that drug abusers would more readily seek treatment. [H. Rept. No. 92-920, 92nd Cong., 2d Sess., 33(1972)]. Implementing regulations issued by the Special Action Office for Drug Abuse Prevention, 21 C.F.R. Part 401, define "patient" as anyone who is or has been interviewed, examined, diagnosed, treated, or rehabilitated in connection with any drug abuse prevention function, and include "research" in the definition of the drug abuse prevention function.

It should be noted that the function of the court order in this scheme is to authorize a disclosure which would otherwise be forbidden, rather than to compel disclosure. The implementing regulations make it clear that the holder of the records *may* disclose the records if so authorized by a court order, but is not obliged to do so.

Discretion to Specify the Conditions for Disclosure. Another pattern of protection is found in Section 1106(a) of the Social Security Act, 42 U.S.C. 1306(a). The section does not deal explicitly with research, but covers any information received by the Department of Health, Education, and Welfare in the course of discharging duties under the Social Security Act. The section provides that no disclosure shall be made "except as the Secretary may by regulations prescribe." Thus, an administrative official is authorized to designate classes of information that may be disclosed, and that may not be disclosed, and to determine when and to whom data may be disclosed. In effect, an administrative official has discretion (which must be exercised in advance in published regulations) to respond to legal process or not.

In all societies men . . . have lived in the interstices of their institutions. They have counted on the mercy of error, ignorance and forgetfulness in their dealings with their fellows and the state. They have often been wrong in so doing—morally and/or factually. But in a world of computers this mercy may not long exist. All our failings and achievements, our credit-worth and our petty delinquencies, our obedience and our defiance, can live in the constant present of the machine.

Donald G. MacRae, "Introduction"
to Spencer's *The Man Versus the State*. *

*(Baltimore: Penguin Books), 1969.

VII

The Social Security Number as a Standard Universal Identifier

Our charter commissioned us to analyze policy and practice relative to the issuance and use of the Social Security number, including prohibitions, restrictions, conditions, or other qualifications on the issuance and use of the number which now exist, or might be imposed to help implement whatever safeguards for automated personal data systems we might recommend.

This particular aspect of our charge stems from growing public concern that the Social Security number will become a standard universal identifier used by all manner of organizations and data systems to establish the identity of individuals, to link records about them, and generally to keep track of them from cradle to grave. This concern also led to the establishment of the Social Security Number Task Force in February 1970, and was reflected in former HEW Secretary Elliot L. Richardson's testimony, in March 1971, before the U.S. Senate Subcommittee on Constitutional Rights, chaired by Senator Sam J. Ervin, Jr.¹

Why do these concerns exist? Are they reasonable? What can be done about them? To answer these questions we must first understand something about identifiers in general and the nature and implications of a standard universal identifier in particular.

¹ *Federal Data Banks, Computers and the Bill of Rights*, Hearings before the Subcommittee on Constitutional Rights of the Committee on the Judiciary, United States Senate, 92nd Congress, 1st Session, February and March 1971, Part I, pp. 775-881.

There are many kinds of personal identifiers. A person's name is an identifier, the most ancient of all, but is not a reliable one, since often it is neither unique nor permanent. Even unusual names may be widely shared, and because of family patterns identical ones are often concentrated in particular localities. Some names change when people marry or divorce, and when children are adopted. Some people are known by different names in different social settings; e.g., itinerants, persons with aliases, and married women who use a maiden name professionally.

To compensate for the unreliability of names as personal identifiers, additional schemes of identification have been devised. These commonly take the form of numeric or alpha-numeric labels that provide the uniqueness and permanence names customarily lack. The reliability thereby achieved is important to record-keeping systems in order to assure accuracy in merging and updating data to be stored about individuals. Usually such labels are established for a single system, but in some instances, a single one may be used in more than one system; for example, in all the record-keeping systems of an organization that maintains different sets of records on a given group of people. If one label is used by separate organizations, such as the Social Security number is for the taxpayer's identification number, a driver's license number, and a school student number, that label may be on its way to becoming a *de facto* universal identifier.

Criteria for a Standard Universal Identifier

A standard universal identifier (SUI) is a systematically assigned label that, theoretically at least, distinguishes a person from all others. If the labels assigned by a universal identification scheme are to fulfill this function, each SUI must meet all the following criteria:

UNIQUENESS. It must be unique for each person. No more than one person can be assigned the same SUI, and each person must have no more than one SUI.

PERMANENCE. It must not change during the life of an individual and should not be re-used after his death until all records concerning him have been retired.

UBIQUITY. Labels must be issued to the entire population for which unique identification is required.

AVAILABILITY. It must be readily obtainable or verifiable by anyone who needs it, and quickly and conveniently regainable in case it is lost or forgotten.

INDISPENSABILITY. It must be supported by incentives or penalties so that each person will remember his SUI and report it correctly; otherwise systems will become clogged with errors.

ARBITRARINESS. It must not contain any information. If it does, e.g., State of issuance, it will be longer than necessary, thus violating the "brevity" criterion (see below). It may also violate the "permanence" criterion if changeable items, such as name or address, are incorporated. Most important, if items of personal information are part of an SUI, they will be automatically disseminated whenever the SUI is used; in our view, this would be undesirable.

BREVITY. It must be as short as possible for efficiency in recognition, retrieval, and processing by man or machine.

RELIABILITY. It must be constructed with a feature that detects errors of transcription or communication.² If the communication of SUIs were done entirely by machine, errors could be minimized through technology, but short of this, there must be protection against the risk of human error in writing or reciting an SUI. For the foreseeable future, the need will continue for people to fill out forms and to report information themselves.

² A possible error-detecting feature is a number (called a check-digit) that can be derived in some way from the identification number and appended to it. For example, a check-digit may be derived by multiplying the first digit of the identification number by 1, the second by 2, the third by 3 (and so on), summing the products of the multiplications, and extracting the digital root of their sum. The identification number 1463, handled this way, produces a check-digit of 3 ($1 \times 1 = 1$, $2 \times 4 = 8$, $3 \times 6 = 18$, $4 \times 3 = 12$; $1 + 8 + 18 + 12 = 39$; $3 + 9 = 12$; $1 + 2 = 3$) which is written at the end of the number to produce 14633. A computer and a human being can each readily verify the accuracy of the number. Transpositions are detectable. "14363," for instance, would be caught as illegitimate, because the correct check-digit for the number 1436 is not 3, but 6 ($1 \times 1 = 1$, $2 \times 4 = 8$, $3 \times 3 = 9$, $4 \times 6 = 24$; $1 + 8 + 9 + 24 = 42$; $4 + 2 = 6$). Most single-digit errors are also detectable, though errors of more than one digit may coincidentally generate valid check-digits and hence not be detectable.

Implications of a Standard Universal Identifier

The advantages of a standard universal identifier, as seen by its proponents, are easier and more accurate updating, merging, and linking of records about individuals for administrative, statistical, and research purposes. According to them, duplication and error in record keeping would be reduced. Individuals, moreover, would be relieved of the need to use many different identifying numbers; an SUI might supplant credit card numbers, personal checking account numbers, driver license numbers, and many other identifiers.

In spite of these practical advantages, the idea of an SUI is objectionable to many Americans. Even in some European countries where SUIs were introduced without opposition a generation or more ago, their use has recently raised fears and anxieties in the population. Many people both feel a sense of alienation from their social institutions and resent the dehumanizing effects of a highly mechanized civilization. Every characteristic of an SUI heightens such emotions.

- The bureaucratic apparatus needed to assign and administer an SUI would represent another imposition of government control on an already heavily burdened citizenry.
- To realize all the supposed benefits of an SUI, mandatory personal identity cards would have to be presented whenever called for. Loss or theft of an SUI card would cause serious inconvenience, and the mere threat of official confiscation would be a powerful weapon of intimidation.
- The national population register that an SUI implies could serve as the skeleton for a national dossier system to maintain information on every citizen from cradle to grave.
- An unchangeable SUI used everywhere would make it much easier for an individual to be traced, and his behavior monitored and controlled, through the records maintained about him by a wide range of different institutions.
- A permanent SUI issued at birth could create an incentive for institutions to pool or link their records, thereby making it possible to bring a lifetime of information to bear on any decision about a given individual. American culture is rich in

the belief that an individual can pull up stakes and make a fresh start, but a universally identified man might become a prisoner of his recorded past.

This Committee believes that fear of a standard universal identifier is justified. Although we are not opposed to the concept of an SUI in the abstract, we believe that, in practice, the dangers inherent in establishing an SUI—without legal and social safeguards against the abuse of automated personal data systems—far outweigh any of its practical benefits. Therefore, we take the position that **a standard universal identifier should not be established in the United States now or in the foreseeable future.**³ The question can surely be re-examined after there has been sufficient experience with the safeguards proposed in this report to evaluate their effectiveness.

The Social Security Number (SSN) as an SUI

But is it not too late to oppose a standard universal identifier? Is not the SSN already a *de facto* SUI? To answer these questions, we must first measure the SSN against the criteria for an SUI given above.

UNIQUENESS. [The SSN is not a unique label. More than 4.2 million people, by the Social Security Administration's own estimates, have two or more SSNs. More serious, although much less prevalent, are the instances in which more than one person has been issued or uses the same SSN.⁴]

³The National Academy of Sciences Computer Databanks Project reached a similar conclusion on the basis of its independent, empirical assessment of the issues involved. See Alan F. Westin and Michael A. Baker, *Databanks in a Free Society* (New York: Quadrangle Books), 1972. pp. 396-400.

⁴"Account number 078-05-1120 was the first of many numbers now referred to as 'pocketbook' numbers. It first appeared on a sample account number card contained in wallets sold . . . nationwide in 1938. Many people who purchased the wallets assumed the number to be their own personal account number. It was reported thousands of times on employers' quarterly reports; 1943 was the high year, with 5,755 wage earners listed as owning the famous number. More recently, the IRS requirement that the Social Security AN [Account Number] be shown on all tax returns resulted in 39 taxpayers showing 078-05-1120 as their number. The number continues to be reported at least 10 times each quarter. There are now over 20 different 'pocketbook' numbers . . ." *Account Number and Employer Contact Manual* (Baltimore, Md.: Social Security Administration), Sec. 121.

PERMANENCE. The SSN is, in almost all cases, permanent for an individual throughout his life.

UBIQUITY. The SSN is nearly universal for adult Americans, much less so for those of high-school age and below.

AVAILABILITY. The SSN of an individual is readily verifiable by the Social Security Administration for some users, and not at all for others. It is regainable from the Social Security Administration by persons who have lost their cards and forgotten their numbers, but not immediately. An individual's SSN, however, is increasingly ascertainable from many sources other than the Social Security Administration.

INDISPENSABILITY. The incentives and requirements to report one's SSN correctly are growing, though in some contexts there are incentives to omit or falsify the number.

ARBITRARINESS. The SSN is not entirely arbitrary; the State of issuance is coded into the number.

BREVITY. The SSN with its nine digits is three places longer than an alpha-numeric label capable of numbering 500 million people without duplication, and two places longer than one that can accommodate 17 billion people. The SSN could therefore be shorter if it were alpha-numeric.

RELIABILITY. The SSN has no check-feature, and most randomly chosen nine-digit numbers cannot be distinguished from valid SSNs. It is thus particularly prone to undetectable errors of transcription and oral reporting.

By our definition, the SSN cannot fully qualify as an SUI; it only approximates one.

The SSN had its genesis in accounting practice and was first known as the Social Security *Account* Number (SSAN). It was established to number accounts for the 26 million people with earnings from jobs covered by the Social Security Act of 1935. Income-maintenance benefits under the Act, though not payable until the retirement or death of a worker, were to be determined on the basis of his record of earnings. Each worker needed a uniquely

identifiable account to which records of his earnings would be posted periodically. Since obviously many would have the same or similar names, it was decided to assign each a unique number to identify his account and assure an accurate record of earnings, which his employer would report both by name and account number.

Name and number were used because standard accounting practice had accustomed people to numbered accounts, and because the technology of the day, notably the punched card machine with its 80-column card, required a short numeric identifier for efficiently adding the records of new transactions to existing master-file records.

Nine digits were chosen to provide for future expansion. A check-feature was not provided because the technology of the day could not cope with it, and manual checking, though possible, was judged too time-consuming to be feasible. The Social Security Administration has developed ingenious error-detection methods, and has improved them over the years to the point where it now neither needs nor desires a check-feature.⁵

Despite the deficiencies of the SSN for purposes other than those for which it was designed, its use is widespread and growing, even where its limitations are recognized. How did this come about? Why is the SSN now so widely used for purposes and in areas unrelated to the Social Security program?

History of the Social Security Number and Its Uses

The original Social Security Act (P.L. 74-271, August 14, 1935) imposed two taxes to finance the program of retirement and survivor benefits to be administered by the Social Security Board. One was a tax as a percentage of wages imposed on employees; the second was a matching tax on employers. To finance the Federal contribution to State programs of unemployment compensation required by the same Act, a tax as a percentage of wages was imposed on employers.

Section 807 of that Act charged the Bureau of Internal Revenue in the Treasury Department with collecting all three taxes. Section 807(b) provided

⁵ *Ibid.*, Sec. 554 ff.

Such taxes shall be collected and paid in such manner . . . (either by making and filing returns, or by stamps, coupons, tickets, books, or other reasonable devices or methods necessary or helpful in securing a complete and proper collection and payment of the tax or in securing proper identification of the taxpayer), as may be prescribed by the Commissioner of Internal Revenue. . . .

The first mention of the SSN in a law or regulation is in a Bureau of Internal Revenue regulation of November 5, 1936 under which an identifying number, called an "account number," was to be applied for by each employee, and assigned by the Postmaster General or the Social Security Board. Each employee was directed to report his number to his employer. Employers were directed to keep records showing the name and number of each employee and to enter employee account numbers on all required tax returns. The regulation provided that "Any employee may have his account number changed at any time by applying to the Social Security Board and showing good reasons for a change. With that exception, only one account number will be assigned to an employee."⁶

It is ironic to discover—though logical and understandable in retrospect—that the first step in the process of extending the use of the Social Security number beyond the purposes of the Social Security program was taken by the Social Security Board itself on January 15, 1937. After the Social Security Act was passed, a question arose about an account numbering system to be used by State agencies established to administer the State unemployment insurance programs. The Board decided that the Social Security number should be used for all workers insured under these programs, rather than have each State agency develop its own identification system. As a result of this decision, many workers not covered by the Social Security program received SSNs for use in State unemployment insurance programs.

For some years after its inception in 1936, there was no substantial use of the SSN other than that required for the Social Security and unemployment compensation programs. Most Americans had not been issued a number, and few organizations felt the need of a numeric identifier for purposes of data processing.

⁶ T.D. 4704, 1 Fed. Reg. 1741 (Nov. 7, 1936); 26 C.F.R. Part 401 (1st ed., 1939).

Although many people are under the impression that use of the SSN for other than Social Security program purposes is forbidden by law, this is not the case and never has been. The impression may in part have arisen from the fact that, for many years, the card bearing one's Social Security Account Number has carried the legend, "NOT FOR IDENTIFICATION." The purpose of this legend is to notify anyone to whom a card might be presented that it cannot be relied upon, by itself, as evidence of the identity of the person presenting it.

In 1943, the Civil Service Commission decided that there should be a numerical identification system for all Federal employees and proposed to the Bureau of the Budget that use of the SSN be authorized for this purpose. This led to the issuance of Executive Order 9397. That order, which is still in effect, provides in part as follows:

WHEREAS certain Federal agencies from time to time require in the administration of their activities a system of numerical identification of accounts of individual persons; and . . .

WHEREAS it is desirable in the interest of economy and orderly administration that the Federal Government move towards the use of a single, unduplicated numerical identification system of accounts and avoid the unnecessary establishment of additional systems;

NOW, THEREFORE, . . . it is hereby ordered as follows:

1. Hereafter any Federal department, establishment, or agency shall, whenever the head thereof finds it advisable to establish a new system of permanent account numbers pertaining to individual persons, utilize exclusively the Social Security account numbers

The order directs the Social Security Board, the predecessor agency of the Social Security Administration, to provide for the assignment of an account number to any person required by any Federal agency to have one, and to furnish the number, or the name and identifying data, pertaining to any person or account number upon request of any Federal agency using the SSAN for a numerical

identification system of accounts under the order. The order also directs that

The Social Security Board and each Federal agency shall maintain the confidential character of information relating to individuals obtained pursuant to the provisions of this Order.

Finally, the order provides for the costs of services rendered thereunder by the Social Security Board to be reimbursed by the agency receiving such services.

Most civil servants had never applied for SSNs because their employment was not covered by the Social Security Act. Since they were not being assigned numbers for Social Security program purposes, the costs had to be paid from funds appropriated for the Civil Service Commission. The Commission, however, was unable to obtain the necessary funds, and so it was not until November, 1961 that the assignment of numbers to Civil Service employees was initiated as an adjunct of the Internal Revenue Service's taxpayer identification program (see below).

The issuance of Executive Order 9397 in 1943 theoretically may have provided the basis for a change in conception of the role of the SSN. However, there is no evidence that it had any practical significance until after the 1961 decision to use the SSN as an individual identifier for Federal tax purposes. It has been suggested that Executive Order 9397 was intended to apply only to instances when Federal agencies seek to number records of financial transactions, and not to numbering other kinds of records, such as employment, attendance, performance, or medical records. The fiscal interpretation follows from the wording of the order which speaks of the efficiency to be gained from "a single . . . system of accounts . . ." To interpret the order as applying to all kinds of Federal agency record systems is arguably beyond the meaning of its language. In any case, it appears that Federal agencies are free to use the SSN in any way they wish, and no instance has come to our attention in which the order has been invoked to compel or limit an agency's use of the SSN.

What many regard as the single most substantial impetus to use the SSN for purposes other than the Social Security program occurred in 1961, when the Internal Revenue Service, after discussions with the Social Security Administration, decided to use

the SSN for taxpayer identification. This decision was implemented by an amendment to the Internal Revenue Code that authorized the Secretary of the Treasury to require each person making "a return, statement, or other document" under the Internal Revenue Code to "include such identifying number as may be prescribed for securing proper identification of such person." The Secretary was also authorized "to require such information as may be necessary to assign an identifying number to any person." The Secretary delegated his authority to the Commissioner of Internal Revenue, who has issued a number of regulations, the combined effect of which may be summarized as follows.

- The taxpayer's identification number for use by individuals (except as employers in a trade or business) is the SSN.
- The SSN for each individual taxpayer and each beneficiary of an estate or trust must be furnished on all tax returns and related statements and documents filed in connection with every tax imposed by the Internal Revenue Code. (A failure to include the number as required on a return gives rise to a civil penalty of \$5, unless the failure to provide the number is due to "reasonable cause." Int. Rev. Code of 1954, Sec. 6676.)
- An individual is obliged to obtain an SSN from the Social Security Administration and furnish it when requested, for purposes of complying with Internal Revenue Service regulations, by any of the following: employers; estates and trusts; corporations and other entities paying dividends; banks, mutual savings and savings and loan institutions; insurance companies; stockbrokers and securities dealers; other entities paying interest; and nominees receiving dividends or interest.

Many other actions of the Federal government have expanded the areas of use of the SSN beyond its original purposes.

- The Treasury Department further expanded use of the SSN in 1963 by requiring its use in registration of all United States transferable and non-transferable securities other than U.S. savings bonds. The following year the requirement for such use of the SSN was applied to Series H savings bonds. The Treasury Department has announced that as of October 1, 1973, the inscriptions on Series E bonds must also include the SSN. (Meanwhile the Treasury has modified its earlier

⁷P.L. 87-397 (Oct. 5, 1961); Internal Revenue Code of 1954, Sec. 6109.

rule that the names of women on savings bond inscriptions be preceded by "Miss," "Mrs.," or other title, by permitting omission of the title if the woman's SSN is included.)

- In a decision dated April 16, 1964, the Commissioner of Social Security approved the issuance of SSNs to pupils in the ninth grade and above, if a school requests such issuance and indicates willingness to cooperate in the effort. The Social Security Administration Claims Manual explains that this decision was made (1) to accommodate requests from school systems "desiring to use the SSN for both automatic data processing and control purposes, so that the progress of pupils could be traced throughout their school lives across district, county, and State lines", and (2) because issuance of SSNs to school children in groups is more orderly, efficient, less costly to the Social Security Administration, and gives better assurance of identification of the children than if students eventually apply for numbers one at a time.
- In June 1965 the Commissioner of Social Security authorized the issuance of an SSN to every recipient of State old-age assistance benefits who did not already have one, in order to establish a more efficient process for exchange of information between these agencies and the Social Security Administration. When the Social Security Act was amended in 1965, to provide hospital and medical insurance (Medicare) administered by the Social Security Administration, it became necessary for most individuals aged 65 and over who did not already have an SSN to obtain one.
- In June 1965 the Civil Service Commission began to add SSNs to the retirement records of their annuitants. This represented an extension of the SSN issuance system started in 1961 for civil service employees.
- Effective January 1, 1966, after consultation with the Social Security Administration, the Veterans Administration began using the SSN as a hospital admission number, and for other record-keeping purposes.
- On April 7, 1966, the Commissioner of Social Security approved the test usage of the SSN by the Division of Indian Health of the Public Health Service to facilitate development and maintenance of comprehensive health histories of Indians from birth to death.

- By memorandum dated January 30, 1967, the Secretary of Defense advised the Social Security Administration of his decision to use the SSN as the service number of all military personnel.
- Pursuant to the Currency and Foreign Transactions Reporting Act (the so-called Bank Secrecy Act), P.L. 91-508, October 26, 1970; 31 U.S.C. 1051-1122, the Treasury Department issued regulations in 1972 requiring banks, savings and loan associations, credit unions, and brokers and dealers in securities to obtain the SSNs of all their customers. The Act requires these financial organizations to maintain records of certain large transactions to facilitate criminal, tax, and regulatory investigations with respect to currency and foreign transactions. The SSNs of individuals required for account records under the regulations will already have been obtained in almost all cases by these financial organizations under regulations of the Internal Revenue Service governing tax reporting. A notable impact has been the requirement to furnish one's SSN to open a checking account.
- Use of the SSN is being promoted by the National Driver Register of the U.S. Department of Transportation. Although the Department of Transportation lacks authority to *require* it, use of the SSN is encouraged by the Register to facilitate matching the records of reports and inquiries it receives. This has led most State motor vehicle departments to collect SSNs from all drivers, and some to shift to the SSN for their driver license identification number.
- The Social and Rehabilitation Service of the Department of Health, Education, and Welfare has for some time been promoting the use of the SSN by States for the identification of individual applicants and beneficiaries under all welfare and social services programs.
- The Congress, in Section 137 of the Social Security Amendments of 1972,⁸ has required the Secretary of HEW to take affirmative measures to issue SSNs to the maximum extent practicable to aliens entitled to work in the United States and "to any individual who is an applicant for or recipient of benefits under any program financed in whole or in part from Federal funds including any child on whose behalf such benefits are claimed by another person." The quoted language of this requirement appears to call for the issuance of an SSN to virtually everyone in America who does not already have one, but the legislative history clearly indicates that such universal enumeration was not intended. The Senate Finance Committee had proposed a

⁸ P.L. 92-603, October 30, 1972; 42 U.S.C. 405.

requirement of affirmative measures for the assignment of SSNs to all children at the time they first enter school, as well as to aliens and all applicants for and recipients of benefits under Federally supported programs. However, the bill was amended in conference. Instead of requiring the Secretary to take affirmative measures to enumerate children at their entrance into school, the Act makes such measures optional, but the Act retains the requirement that numbers be assigned to aliens, and to applicants and recipients of benefits. Although the legislation does not specify any uses to be made of SSNs issued pursuant to its mandate, the legislative history indicates that Congress intended them to be available for use in preventing aliens from working illegally and public assistance beneficiaries from receiving duplicate or excessive payments.

Review of the Federal actions described above (which do not by any means constitute an exhaustive list makes it clear that *the Federal government itself has been in the forefront of expanding the use of the SSN*. All these actions have actively promoted the tendency to depend more and more on the SSN as an identifier—of workers, taxpayers, automobile drivers, students, welfare beneficiaries, civil servants, servicemen, veterans, pensioners, and so on.

(If use of the SSN as an identifier continues to expand, the incentives to link records and to broaden access to them are likely to increase.) Until safeguards such as we have recommended in Chapters IV, V and VI have been implemented, and demonstrated to be effective, there can be no assurance that the consequences for individuals of such linking and accessibility will be benign. At best, individuals may be frustrated and annoyed by unwarranted exchanges of information about them. At worst, they may be threatened with denial of status and benefits without due process, since at the present time record linking and access are, in the main, accomplished without any provision for the data subject to protest, interfere, correct, comment, and, in most instances, even to know what linking of which records is taking place for what purposes.

Although few people have flatly proposed that an SUI be mandated for all Americans, there is a strong tendency for authorities in government and industry to make decisions that, taken collectively, are likely to lead to the establishment of an SUI. There is an increasing tendency for the Social Security number to be used as if it were an SUI. Even organizations selecting a

single-system personal identifier are likely to choose the SSN "because it is available," or for efficiency and convenience. There are pressures on the Social Security Administration to do things that make the SSN more nearly an SUI, such as issue more SSNs than the Social Security program requires, for purposes wholly unrelated.

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 or government-supported automated personal data systems.⁹ What is needed is a halt to the drift toward an SUI and prompt action to establish safeguards providing legal sanctions against abuses of automated personal data systems.] The recommendations in the following chapter are directed toward that end.

⁹One notable attempt to establish a standard for the identification of individual Americans for purposes of information exchange was that offered by a committee of the American National Standards Institute (ANSI) in 1969. The standard, as proposed, consisted in part of an individual's SSN; opposition to that feature in particular led in 1972 to official withdrawal of the standard from further consideration pending resolution of the issues that are covered by this report.

*The Unknown Citizen
(To JS/07/M/378
This Marble Monument
Is Erected by the State)*

*He was found by the Bureau of Statistics to be
One against whom there was no official complaint,
And all the reports on his conduct agree
That, in the modern sense of an old-fashioned word, he
was a saint,
For in everything he did he served the Greater Community.
Except for the War until the day he retired
He worked in a factory and never got fired,
But satisfied his employers, Fudge Motors, Inc.
Yet he wasn't a scab or odd in his views,
For his Union reports that he paid his dues,
(Our report on his Union shows it was sound)
And our Social Psychology workers found
That he was popular with his mates and liked a drink.
The Press are convinced that he bought a paper every day
And that his reactions to advertisements were normal in
every way.
Policies taken out in his name prove that he was fully insured,
And his Health-card shows he was once in hospital but left
it cured.
Both Producers Research and High-Grade Living declare
He was fully sensible to the advantages of the Instalment Plan
And had everything necessary to the Modern Man,
A phonograph, a radio, a car and a frigidaire.
Our researchers into Public Opinion are content
That he held the proper opinions for the time of year;
When there was peace, he was for peace; when there was war,
he went.
He was married and added five children to the population,
Which our Eugenicist says was the right number for a parent of
his generation,
And our teachers report that he never interfered with
their education.
Was he free? Was he happy? The question is absurd:
Had anything been wrong, we should certainly have heard.*

W. H. Auden

Copyright © 1940 and renewed 1968 by W. H. Auden. From *Collected Shorter Poems, 1927-1957*. Reprinted by permission of Random House, Inc.

VIII

Recommendations Regarding Use of the Social Security Number

Until safeguards against abuse of automated personal data systems have become effective, constraints should be imposed on the use of the SSN. After that, the question of SSN use might properly be reopened.

We recommend that Federal policy with respect to use of the SSN be governed by the following general principles.

First, uses 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 the automated personal data systems that would be affected by the proposed use of the SSN.

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 light of these principles, we make specific recommendations with respect to the individual's right to refuse to disclose his SSN, issuance of SSNs, constraints on use or dissemination of SSNs, and prohibition of non-data-processing uses of the SSN. Ideally, (Congress should review all present Federal requirements for use of the SSN to determine whether the existing requirements should be continued, repealed, or modified.) In this chapter, we recommend several modifications that would apply to all SSN requirements now in force.

how do you use the SSN? why?

Specific Recommendations on the Social Security Number

RIGHT OF AN INDIVIDUAL TO REFUSE TO DISCLOSE THE SOCIAL SECURITY NUMBER

As indicated in Chapter VII, increasing demands are being placed on individuals to furnish an SSN in circumstances when use of the SSN is not required by the Federal government for Federal program purposes. For example, the SSN is demanded of individuals by State motor vehicle departments, by public utility companies, landlords, credit grantors, schools, colleges, and innumerable other organizations.

Existing Federal law and Social Security regulations are silent on such uses of the SSN. They provide no clear basis for keeping State and local government agencies and private organizations from demanding and using the number. As a practical matter, disclosure of one's SSN has been made a condition for obtaining many

benefits and services, and legal challenges to this condition under State law have been almost uniformly unsuccessful.

If the SSN is to be stopped from becoming a *de facto* SUI, the individual must have the option not to disclose his number unless required to do so by the Federal government for legitimate Federal program purposes, and there must be legal authority for his refusal. Since existing law offers no such clear authority, we recommend specific, preemptive, Federal legislation providing:

- (1) That an individual has the 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.
- (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.

ISSUANCE OF SOCIAL SECURITY NUMBERS

The report of the Social Security Number Task Force¹ identified the need to improve the integrity of the SSN for some uses now required by Federal law. Steps have been initiated during the last two years to decrease the likelihood that any individual will be assigned more than one SSN without the knowledge of the Social Security Administration. They include: improved procedures for verifying the identity of each applicant for an SSN; issuance of SSNs only from the central office of the Social Security Administration rather than from its 1,000 field offices; implementation of a process that will provide comprehensive, automated screening of applications for SSNs; and the establishment by Section 208 of the Social Security Act² of a penalty for fraudulently furnishing false

¹ *Social Security Number Task force: Report to the Commissioner* (Baltimore, Md.: U.S. Social Security Administration), 1971.

² As provided by Section 130 of the Social Security Amendments of 1972, P.L. 92-603, October 30, 1972; 42 U.S.C. 408.

information regarding one's identity in order to obtain an SSN. There is good reason to expect that the combined effect of all these actions will be to improve significantly the integrity of the SSN.

Enumeration of School Children. The Social Security Number Task Force recommended that the Social Security Administration "should embark on a positive program of enumerating [issuing SSNs to] school children at the ninth-grade level, with concurrent establishment of proof of age and identity." We have given long and careful thought to this recommendation. Our first inclination was flatly to oppose it as an action that would promote the use of the SSN as a *de facto* SUI. After further deliberation, and exploration of relevant issues with the Commissioner of Social Security, we decided to endorse the Task Force recommendation with two important qualifications. Specifically, 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.

Children in the ninth grade have reached the age when they are likely to seek part-time or summer employment and need an SSN for Social Security program and Federal income tax purposes. Indeed, many young people obtain SSNs for such purposes before they reach ninth grade. Under Section 137 of the Social Security Amendments of 1972, many children who receive certain Federal cash benefits will also be assigned SSNs before they reach ninth grade. Since a program of ninth-grade enumeration is likely to be consistent with the needs and convenience of most young people, it is not likely to seem coercive. Moreover, our recommendation is designed to prevent any coercion.

Both the Task Force Report and the Commissioner of Social Security have indicated that a program of ninth-grade enumeration would offer the Social Security Administration an opportunity to inform students about the Social Security program and their rights

and responsibilities in relation to it. We urge that any such student briefings include information about their rights and responsibilities with respect to uses of the SSN. We also note the observations made in the Task Force Report, and reiterated by the Commissioner of Social Security, that ninth-grade enumeration is advantageous to the Social Security Administration on a cost-benefit basis.

Finally, our inquiries and discussions with Social Security Administration representatives convinced us that a positive program of ninth-grade enumeration would contribute significantly to enhancing the integrity of the SSN. The contribution to this end might appear somewhat greater if the program enumerated children at the time of their first enrollment in school, as authorized by the Congress in Section 137 of the Social Security Amendments of 1972. However, we strongly recommend

(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.

A positive program of issuing SSNs to all children at school entry has little to recommend it. It would almost surely seem coercive, since the proportion of children in kindergarten or first grade who need an SSN is small. These children are too young for a significant educational contact with the Social Security program. Most important, such a mass enumeration program would be a very significant further step toward making the SSN a *de facto* standard universal identifier—a step there are no compelling reasons to take.

Enumeration of Beneficiaries of Federally Funded Programs. As we noted in Chapter VII (pp. 120-121), Section 137 of the Social Security Amendments of 1972 requires the Secretary of HEW to take affirmative measures to issue the SSN as widely as practicable.

to any individual who is an applicant for or recipient of benefits under any program financed in whole or in part from Federal funds including any child on whose behalf such benefits are claimed by another person.

This provision, read literally, could well provide the authority for establishing a standard universal identifier. Yet as we understand it,

this provision was included in the legislation in the narrow context of improving the administration of public assistance programs. It is a technical provision in a large and complicated piece of legislation (the printed Public Law runs to 165 pages) in which other very controversial issues occupied the attention of the Congress and the public. This particular provision was not the subject of public hearings.

The conditions under which Section 137 became law did not allow for adequate consideration of an action that has the potential of driving America toward an SUI. We therefore believe that the Secretary has an obligation to use the authority granted in Section 137 only in the most limited way consistent with the mandate—as a tool for improving the administration of public assistance programs. The potential consequences are too dangerous to allow an SUI to be established without wide and careful public consideration and full assessment of the potential consequences.

Specifically, we recommend

(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.

We further recommend

(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.

[We would stress once again that the SSN in its present form is not a satisfactory standard universal identifier. Even with the steps that have been taken to improve the integrity of the SSN, the SSN cannot provide a guarantee of identity unless it is coupled with some stable feature of physical identification, such as fingerprints. In its present form, therefore, adoption of the SSN as an SUI would not lead to all the advantages of improved program administration that proponents of its widened use anticipate, e.g., to “identify” welfare beneficiaries.

If the Committee had to choose today between a *true* SUI, complete with fingerprinted identification cards on the one hand, and something less than ultimate efficiency in the administration of public assistance programs on the other, we would rather risk the latter; we think the American public would too. The steps being taken to strengthen the integrity of the SSN can lead to significant improvement in the administration of public assistance, while our recommendations will check the drift of the SSN toward becoming a *de facto* SUI. Until effective safeguards against the abuse of computer-based personal data systems have been established, and until there has been full public debate of the desirability of an SUI, this is the point at which the situation must be held in check.

CONSTRAINTS ON USE AND DISSEMINATION OF SOCIAL SECURITY NUMBERS

Recommendations (8)-(10) below are designed to limit uses of the SSN to those necessary to carry out Federal government purposes for which there is a legal requirement that the SSN be obtained and recorded, and to discourage all practices that substantially increase the circulation of individual SSNs together with the names of their holders.

Recommendation (8) is intended to constrain the behavior of organizations and persons that are legally required to obtain and record the SSN for Federal purposes, but which use the SSN in other ways that constitute virtual public dissemination of SSNs along with names of the individuals to whom they belong. Among the many uses of the SSN that this recommendation is designed to abate are its use as an employee identification number, a patient identification number, a student identification number, a customer identification number, a driver identification number, and as the primary organizing element in the record-keeping system of any non-Federal organization. Although such uses may be convenient, they are not necessary. Under present circumstances, moreover, they increase the circulation of SSNs, thereby inviting unconstrained linking of record-keeping systems. Accordingly, 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 government purposes for which it was required to be obtained and recorded. This prohibition should be established by a specific and preemptive act of Congress.

This recommendation stems in part from observing that the Social Security Administration treats the SSN with the same confidentiality as the data in its records of Social Security accounts. Access to Social Security data is governed by Section 1106 of the Social Security Act and Regulation No. 1 of the Social Security Administration. The result is that the Social Security Administration will disclose an individual's SSN *only to those third persons and organizations permitted by law to obtain SSA record data*. The Social Security Administration and the Internal Revenue Service each require organizations to obtain and use the SSNs of individuals for various Federal program purposes. In principle these agencies should require such organizations to treat the SSN with the same confidentiality as the Social Security Administration does. Regrettably, however, there appears to be no legal authority to support the imposition of such a requirement. Recommendation (8) would establish such authority.

Recommendation (8), coupled with recommendations (1) and (3) (pp. 125-126, above), would also diminish the risk of nuisance, frustration, and possible serious disadvantage resulting from the use of an individual's SSN to impersonate him. One use of the SSN that appears to be proliferating is as a password, or authenticator of identity, when an individual's name alone is thought insufficient; e.g., in credit-card purchasing and check-cashing. Such use is not necessary, just convenient, and can be risky, since the widespread circulation of SSNs makes them increasingly ascertainable by anyone wishing to impersonate another.

An example from our own experience will illustrate the problem. We met on a Saturday in a conference room in a government facility. Security procedures required us to give names and SSNs from a telephone located outside the locked main entrance to a guard who was out of sight inside the building. The guard had earlier been furnished with a list of our names and SSNs. Given the wide dissemination of SSNs, we were impressed by how easily someone

could have impersonated any one of us to gain admittance to the building.

One may treat this example lightly, but the principle is important. As long as the SSN of an individual can be easily obtained (some organizations list the SSNs of their employees or members in published rosters), both individuals and the organizations that use it as a password are vulnerable to whatever harm may result from impersonation.

Recommendations (9) and (10) are intended to constrain the provision of "SSN services" by the Social Security Administration. The phrase, "SSN services," is defined in the Social Security Number Task Force Report as including

enumeration, or issuing numbers to individuals who do not have them; *validation*, or confirming that the number an organization has on file for an individual is the same as the number that appears for him in SSA records; *correction*, or supplying the proper number from SSA files when an individual has alleged an incorrect number; and *identification*, or supplying a number from SSA's files to match a particular name, a name to match a number, or vice-versa [sic].³

The Task Force report recommends that SSN services be provided by the Social Security Administration (i) "to public and private organizations using the SSN for health, welfare, or educational purposes" and (ii) to facilitate research activities.

Although we recognize the spirit of cooperation that prompted the Task Force position, we believe that the effect of the recommendations would unnecessarily spread use of the SSN. Our recommendations limit SSN services even more narrowly than the Task Force recommendations.

We recommend

(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; and

³Op. cit. pp. 26-27

(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.

These recommendations distinguish between use of the SSN for record-keeping purposes and its use for research activities. SSN services must not be provided to aid an organization's record-keeping, except to the extent necessary to enable the organization to fulfill requirements associated with its Federally imposed obligations to collect and record the number. Our recommendation (8) would prohibit organizations from using the SSN beyond this limit, and the Social Security Administration would be obliged to refrain from providing SSN services in cooperation with a violation of the prohibition. As an interim measure, the Social Security Administration should limit SSN services as though recommendation (8) were in force. The limitation must apply to all cases, including requests from organizations that provide health, education, and welfare services.

The effect of our recommendations may be illustrated by a case discussed in the Social Security Number Task Force Report.⁴ A State mental health service requested SSN services from the Social Security Administration to enable it to use the SSN as the patient identification number in a new computerized record-keeping system. It evidently wanted to use the number for general administrative record keeping; such a use is not legally required for any Federal program purpose. The mental health service is obligated to use the SSN to report the earnings and income taxes of its own employees; it might also need to obtain and use the SSNs of some of its patients to comply with record-keeping requirements of Federal benefit programs mandated by the Social Security Act, e.g., Medicare. However, its Federally required SSN uses do not extend to using the SSN for all patient record keeping, and the mental

⁴Ibid., pp. 24-25.

health service can clearly create its own identification code to track patients.

If the SSN Task Force recommendations were to be followed in this case, the Social Security Administration would provide SSN services to the mental health service for all its patient record keeping (to simplify the service's reporting of unduplicated patient counts to HEW's National Institute of Mental Health). Under our recommendation, by contrast, the Social Security Administration would not provide SSN services, and the SSN would, therefore, not be spread by various uses of mental health service records and thus become available for still other uses.

Recommendation (10) recognizes the interest in providing SSN services in support of various kinds of evaluation and research activities. There is no reason why this cannot be done without adding to the unnecessary spread of the SSN for record-keeping and data-processing activities or to SSN dissemination of the sort we wish to curtail.

In the case discussed above, suppose that the State mental health service proposes to conduct studies of the effectiveness of its services, and that knowing the SSNs of its patients, and having SSN services, might help in some way. Lacking any Federal requirement to use the SSN for evaluation research, the mental health service could not compel disclosure of patients' SSNs for that purpose. However, for all patients' SSNs voluntarily disclosed with informed consent, our recommendation (10) would permit the Social Security Administration to provide SSN services.

PROHIBITION OF NON-DATA-PROCESSING USES OF THE SOCIAL SECURITY NUMBER

The SSN is sometimes used for a purpose having nothing to do with identification, record keeping, or data processing. While these uses do not directly contribute to unfair information practices, they have other undesirable effects. Consider these examples.

- "Lucky number" contests in which an SSN is drawn, and its holder is awarded some prize. This is objectionable because it may induce people to try to obtain extra SSNs to increase their chances of winning, and because it trivializes the SSN.

- Various items of merchandise, such as wallets, sold with a number-bearing facsimile Social Security card enclosed. This is how one such sample number noted in Chapter VII⁵ came to be used by more than five thousand people. There are undoubtedly other difficulties that have not yet come to light. We understand that such practices are abating as a result of years of intensive (and expensive) fieldwork by the Social Security Administration which, however, has no legal authority to prevent them.

- "Skip-tracing" efforts in which, to quote a Social Security Administration manual,

[d]ebt or tracing organizations occasionally use special correspondence techniques to obtain information from an individual owing money. Some mail out postcards showing a false [SSN] and asking "Is this your Social Security number? If not, call the number listed below to correct this matter."

This is blatantly deceptive and violates reputable business practice. It may also lead people to think that the Social Security Administration is somehow cooperating with skip-tracers.

Such spurious uses of Social Security cards and SSNs tend to interfere with appropriate uses of the SSN and to confuse the public about its proper purposes. They also complicate the work of the Social Security Administration. Accordingly, we recommend

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

⁵ Note 4, p. 112, above.

IX

Action Agenda for the Secretary of Health, Education, and Welfare

The charter directs us to specify the steps that must be taken to put our recommendations into effect. We have done so in this chapter. For each action outlined below, the chapter and pages of the report where the corresponding recommendation is discussed are indicated.

Legislation

We have made a number of recommendations that require the submission of legislative proposals to the Congress as follows.

- To establish a code of fair information practice for all automated personal data systems maintained by agencies of the Federal government or by organizations within reach of the authority of the Federal government. The code should embody safeguard requirements for both administrative systems and systems used exclusively for statistical reporting and research, and should provide injunctive relief as well as civil and

penal sanctions for violation of the code [Ch. IV, pp. 50, 53-64; Ch. V, pp. 86-87; Ch. VI, pp. 97-102].

- To establish protection against compulsory disclosure through legal process for identifiable personal data used exclusively for statistical reporting and research [Ch. VI, pp. 102-106];
- To amend the Freedom of Information Act to require that an agency obtain the consent of an individual before disclosing data about him in identifiable form [Ch. IV, pp. 64-66].
- To protect individuals against unauthorized use of the Social Security number by providing that:
 - (i) an individual shall have the right not to disclose his Social Security number unless specifically required to do so by Federal statute [Ch. VIII, pp. 125-126];
 - (ii) any oral or written request made to an individual for his Social Security number shall be accompanied by a clear statement of the legal basis for the request [Ch. VIII, pp. 125-126];
 - (iii) an individual shall have a right to redress if his lawful refusal to disclose his Social Security number results in the denial of a benefit, or the threat of such denial [Ch. VIII, pp. 125-126];
 - (iv) any organization or person required by Federal law to obtain and record the Social Security number of an individual shall be prohibited from using or disclosing it without the individual's informed consent, except as may be necessary to the Federal purposes for which the number was obtained and recorded [Ch. VIII, pp. 130-132].
- To prohibit any person or organization from using any Social Security number, or any number represented as a Social Security number, for promotional or commercial purposes [Ch. VIII, pp. 134-135].
- To amend Section 609(a) of the Fair Credit Reporting Act
 - (i) to give an individual the right to inspect personally the records that any consumer-reporting agency maintains

about him, and to copy their contents or have copies made [Ch. IV, pp. 66-70];

(ii) to delete the exceptions from disclosure to an individual now permitted for medical information and sources of information used in investigative consumer reports [Ch. IV, pp. 70-71].

Action by the Secretary to initiate these legislative proposals should be taken in concert with the Attorney General, the Secretary of the Treasury, and the Chairman of the Federal Trade Commission, as appropriate.

Administrative Action

Many of our recommendations can be implemented by the issuance of regulations or administrative guidelines.

Regulations should be issued:

- To make applicable all the safeguard requirements for automated personal data systems to all systems within the Department [Ch. IV, pp. 50-64; Ch. V, pp. 85-87; Ch. VI, pp. 95-102].
- To make applicable all the safeguard requirements for automated personal data systems to all systems that can be reached through grant, contract, or other relations with the Department [Ch. IV, p. 50; Ch. V, p. 86; Ch. VI, p. 96].
- To amend the Department's regulation under the Freedom of Information Act to provide that the consent of an individual shall be obtained before disclosing any data about him in identifiable form [Ch. IV, pp. 65-66].

Administrative guidelines should be issued:

- Establishing procedures for rigorous and thorough evaluation of
 - (i) any proposal to create or expand any automated personal data system within the Department [Ch. IV, pp. 51-52];

(ii) any proposal to use administrative personal data for statistical reporting or research [Ch. V, pp. 82-86]; and

(iii) any proposal that would tend to require the creation or expansion of an automated personal data system outside the Department in response to requirements or needs of programs and activities of the Department [Ch. IV, p. 52].

- Requiring that a regulation, with notice of proposed rule making, be issued by the Department before taking any action that would tend to require a State, locality, or other grantee to create or expand an automated personal data system [Ch. IV, p. 52].
- Providing for the publication annually of a compilation of the public notices of all automated personal data systems maintained within the Department [Ch. IV, pp. 57-58; Ch. VI, pp. 99-101].
- Directing the Social Security Administration:
 - (i) to undertake a positive program to issue Social Security numbers 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 a Social Security number in connection with such a program [Ch. VIII, 127-128];
 - (ii) to undertake no positive program of issuing Social Security numbers to children below the ninth-grade level [Ch. VIII, p. 128];
 - (iii) to limit affirmative measures taken to issue Social Security numbers pursuant to subparagraph (B) (i) (II) of Section 205 (c) (2) 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 [Ch. VIII, pp. 128-130];
 - (iv) to provide SSN services only to organizations or persons required by Federal law to obtain or record the Social Security number, and then only as necessary to fulfill the

purposes for which the number is required to be obtained or recorded; or in aid of research activities whose design incorporates rigid safeguards to protect the confidentiality of personal data, including the Social Security number [Ch. VIII, pp. 132-134].

(v) to monitor all future legislative proposals dealing with the Social Security number and to recommend actions to be taken by the Secretary to assure that such proposals will be enacted only after full and careful consideration in well advertised hearings that elicit substantial public participation [Ch. VIII, pp. 129-130].

Additional Action

In addition to the steps necessary to put our recommendations into effect, there are some further steps the Department can take to assure that the goals of the recommendations are fully achieved. These include:

- Communicating opposition to any proposal for 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 or government-supported automated personal data systems;
- Making comments on proposed Federal legislation having implications for personal privacy in record keeping which will seek to assure incorporation in such legislation of safeguard requirements of the kind recommended in this report for all automated personal data systems;
- Encouraging attention in all forms of educational activity to the individual citizen's stake in his personal privacy, to the practical exercise of his rights with respect to the records maintained about him, and to the social impact of computer-based record-keeping systems;
- Supporting research on the use and impact of computer-based record-keeping systems in such areas as education,

health services delivery, public assistance, juvenile delinquency prevention, and community mental health;

- Encouraging the development of standards of ethical behavior and professional competence for data-processing personnel;
- Enhancing the capacity of the Federal government to design and develop computer-based record-keeping systems without reliance on outside specialists;
- Monitoring the application of the safeguard requirements to determine whether they are having their intended effect and, most important, whether they are themselves a source of any adverse social consequences;
- Cooperating with the States in developing uniform State legislation to establish the recommended code of fair information practice for all automated personal data systems that would not be reached by Federal legislation. Among the organizations through which such cooperation might be undertaken are the National Conference of Commissioners on Uniform State Laws, the Advisory Commission on Intergovernmental Relations, the Council of State Governments, the National Governors Conference, the National Legislative Conference, and the National Conference of State Legislative Leaders.
- Urging the Office of Management and Budget to direct all Federal agencies to require their grantees and contractors to operate automated personal data systems with all the safeguards we recommend for systems supported by the Department. In the interest of convenience and simplicity for grantees and contractors, the Office of Management and Budget might prescribe government-wide grant and contract conditions incorporating the safeguard requirements we recommend, just as it now prescribes conditions in such areas as intergovernmental planning and financial management. While such action may not be feasible until there has been some experience in applying the safeguard requirements, we would expect to see the Department take a lead role in promoting

uniform, government-wide safeguard requirements for automated personal data systems of Federal grantees and contractors.

Organizational Responsibility

Responsibility for taking the actions necessary to implement our recommendations will have to be assigned to many officials of the Department who are already burdened with other duties. They will need guidance and assistance. The Secretary will need to designate someone who can devote substantial time and effort to assuring that these actions are taken in a timely and effective fashion. Therefore, an official in the Office of the Secretary should be given responsibility to serve as a combination advisor, monitor, and catalyst to assure that the concerns addressed in this report receive continuing attention, and specifically, to assure that automated personal data systems within the Department, and within grantee and contractor agencies, are operated in accordance with the safeguards we recommend. This official should have adequate authority, staff, and support to conduct these activities effectively.

This official should be directed to embark on a positive program of heightening concern within the Department for the issues raised in this report. This program should reach to all who now do, or are apt in the future, to use, direct, or contribute to the use or development of automated personal data systems, at all Civil Service grade levels and in all operating agencies.

Immediate Action

We expect that the Secretary may wish to have the report reviewed by many key officials of the Department, including the heads of each of the Department's operating agencies. Following such a review, a detailed plan to carry out the foregoing action agenda will have to be formulated.

Once such a plan has been adopted, responsibility will have to be assigned to someone to oversee its execution. To start this process we recommend that the Secretary:

- Assign responsibility for distributing the report for review to the Executive Secretary of the Department; and
- Assign responsibility for preparing a detailed plan to carry out the action agenda to an official in the Office of the Secretary.

Appendices

Appendix A

Meetings and Activities of the Secretary's Advisory Committee on Automated Personal Data Systems February 27, 1972 - March 31, 1973

The effective date of formation of the Committee was February 27, 1972, the date on which former HEW Secretary Elliot L. Richardson approved its Charter. The Committee's first meeting was held on April 17 and 18, 1972, at the Fogarty International Center, National Institutes of Health, Bethesda, Maryland. Prior to the second meeting of the Committee, Frances Grommers, M.D., of Boston, Massachusetts, was appointed Chairman. In January 1973, Dr. Grommers was succeeded as Chairman by Dr. Willis H. Ware of the Rand Corporation, Santa Monica, California.

The names and affiliations of the individuals who made presentations to the Committee at its nine meetings are listed below. An unedited transcript of each meeting has been deposited in the Department of Health, Education, and Welfare Library.

FIRST MEETING, APRIL 17-18, 1972

David B.H. Martin, Special Assistant to the Secretary of HEW

Explanation of background and aims of Committee.

**Gerald L. Davey, President and Chief Executive Officer, Medlab
Computer Services, Inc.**

Discussion of record-keeping practices and use of Social Security number in credit-reporting industry.

James C. Impara, Administrator of Educational Accountability, Department of Education, State of Florida

Explanation of high school student records data systems of State of Florida.

Patricia J. Lanphere, Assistant Supervisor, Bureau of Services to Families and Children, Department of Institutions, Social and Rehabilitative Services, State of Oklahoma

Explanation of data systems used by her department.

Prof. Arthur R. Miller, Harvard Law School

Discussion of the law of privacy.

Robert A. Knisely, Chairman, Urban Information Systems Inter-agency Committee (USAC); Director, Division of Community Management Systems, Department of Housing and Urban Development

Discussion of integrated municipal information systems.

Arthur E. Hess, Deputy Commissioner, Social Security Administration, DHEW

Discussion of use of the Social Security number and the confidentiality of Social Security Administration records.

Thomas S. McFee, Deputy Assistant Secretary for Management Planning and Technology, DHEW

Discussion of the procedures under the Federal Reports Act of 1942 governing the collection of information by the Federal government.

Carole W. Parsons, Staff Associate, Division of Behavioral Sciences, National Academy of Sciences – National Research Council

Discussion of activities and organization of the NAS-NRC Advisory Committee on Problems of Census Enumeration.

SECOND MEETING, MAY 18-19, 1972

Gerald L. Boyd, Deputy Director, Office of Family Benefits Planning, DHEW

Discussion of planning, with emphasis on data systems, for the administration of benefit programs proposed in H.R. 1 (welfare reform legislation).

Bernard H. Kroll, Head, Section on Systems Design and Data Processing, Office of Biometry, National Institute of Neurological Diseases and Stroke (NINDS), National Institutes of Health, DHEW

Discussion of the Perinatal Collaborative Study of NINDS.

Anthony J.J. Rourke, Jr., M.D., Chief, Office of Clinical and Management Systems, Clinical Center, National Institutes of Health, DHEW

Discussion of the Clinical Center's automated personal data systems.

Joseph D. Naughton, Chief, Computer Center Branch, Division of Computer Research and Technology, National Institutes of Health, DHEW

Presentation of the National Institutes of Health Computer Center.

Kenneth A. McLean, Professional Staff Member, Committee on Banking, Housing, and Urban Affairs, U.S. Senate

Discussion of the Fair Credit Reporting Act.

Mario L. Juncosa, Physical Sciences Department, The Rand Corporation

Rein Turn, Information Sciences and Mathematics Department, The Rand Corporation

Discussion of current studies by The Rand Corporation on security of data systems.

Harry S. White, Jr., Associate Director, Center for Computer Standards, National Bureau of Standards, Department of Commerce

Discussion of activities of the American National Standards Institute (ANSI) in development of standard for identification of individuals proposed by ANSI.

Lawrence M. Baskir, Chief Counsel and Staff Director, Constitutional Rights Subcommittee, Committee on the Judiciary, U.S. Senate

Discussion of the Subcommittee's activities, concerns, and hearings on *Federal Data Banks, Computers and the Bill of Rights*.

THIRD MEETING, JUNE 15-17, 1972

Roye L. Lowry, Clearance Officer, Statistical Policy Division, Office of Management and Budget, Executive Office of the President

Thomas S. McFee, Deputy Assistant Secretary for Management Planning and Technology, DHEW

Arthur Benner, Chief, Forms and Records Management Section, Division of Operating Facilities, Office of Administration, Social Security Administration, DHEW

Discussion of the procedures under the Federal Reports Act of 1942 governing the collection of information by the Federal government.

Michael A. Liethen, Office of the Chancellor - Legal Counsel, University of Wisconsin, Madison

Discussion of record-keeping activities of the University of Wisconsin, Madison.

Walter M. Carlson, Corporate Marketing Consultant, International Business Machines Corporation, and Past President of the Association for Computing Machinery

Discussion of IBM's data security program.

Discussion of standard for identification of individuals proposed by the American National Standards Institute (ANSI).

Juan A. Anglero, Assistant Secretary for Planning and Development, Department of Social Services, Commonwealth of Puerto Rico

Discussion of decentralization of data systems and the differential impact of data systems according to socio-economic and ethnic status.

Prof. Joseph Weizenbaum, Department of Electrical Engineering, Massachusetts Institute of Technology

Discussion of linkages, centralization, and irreversible social consequences of data systems.

Prof. Arthur R. Miller, Harvard Law School

Discussion of the right of due process.

Lois L. Elliott, Director, Management Information, Bureau of Education for the Handicapped, Office of Education, DHEW

Discussion of the Uniform Migrant Student Record Transfer System.

George Friedman, Assistant Bureau Director, Systems, Bureau of Data Processing, Social Security Administration, DHEW

Discussion of data collection activities of the Social Security Administration, procedures for issuance of the Social Security number, and costs of maintaining data files.

Gerald L. Davey, President and Chief Executive Officer, Medlab Computer Services, Inc.

Outline of plans for proposed study of costs of creating and maintaining selected types of automated personal data systems.

FOURTH MEETING, JULY 24-26, 1972

Earle P. Shoub, Deputy Director, Appalachian Laboratory for Occupational and Respiratory Diseases, Environmental Health Service, DHEW

Edward J. Baier, Deputy Director, National Institute for Occupational Safety and Health, Health Services and Mental Health Administration, DHEW

Discussion of the Morgantown, West Virginia Medical X-Ray Examination System.

Fred Sachs, Assistant Commissioner for Program Management, Rehabilitation Services Administration, Social and Rehabilitation Service, DHEW

Wesley Grier, Chief, Division of Program Surveys and Statistics, National Center for Social Statistics, DHEW

Nathan Lesowitz, Chief, Statistical Branch, Rehabilitation Services Administration, Social and Rehabilitation Service, DHEW

Discussion of the Vocational Rehabilitation Case Service Report System.

Prof. Ithiel de Sola Pool, Department of Political Science, Massachusetts Institute of Technology

Discussion of the benefits and possible adverse consequences flowing from applications of the methods and tools of the social sciences.

Dr. Robert R. J. Gallati, Director, New York State Identification and Intelligence System

Adam D'Alessandro, Deputy Director, New York State Identification and Intelligence System

Discussion of New York State Identification and Intelligence System (NYSIIS).

Harry P. Cain II, Director, Office of Program Planning and Evaluation, National Institute of Mental Health, Health Services and Mental Health Administration, DHEW

Irving Goldberg, Chief, Evaluation Studies Section, Biometry Branch, National Institute of Mental Health, Health Services and Mental Health Administration, DHEW

Jean Warthen, Director, Center for Health Statistics, Maryland Department of Mental Hygiene

Discussion of the Maryland Psychiatric Case Register System.

Allan Lichtenberger, Chief, Educational Data Standards Branch, National Center for Educational Statistics, DHEW

John Putnam, Education Program Specialist, Educational Data Standards Branch, National Center for Educational Statistics, DHEW

Ivan N. Seibert, Education Program Specialist, Educational Data Standards Branch, National Center for Educational Statistics, DHEW

Charles T. Roberts, Education Program Specialist, Educational Data Standards Branch, National Center for Educational Statistics, DHEW

Discussion of Chapter 6 of Office of Education Handbook V, "Standard Terminology for Pupil Information in Local and State School Systems."

St. John Barrett, Deputy General Counsel, DHEW

William H. Small, Vice President, CBS News

Samuel J. Archibald, Executive Director, Fair Campaign Practices Committee, Inc.

Discussion of the Freedom of Information Act.

Marvin Schneiderman, Acting Associate Scientific Director, Demography, National Cancer Institute, National Institutes of Health, DHEW

Harvey Geller, Head, Special Cancer Survey Section, Biometry Branch, National Cancer Institute, National Institutes of Health, DHEW

Theodore Weiss, Head, Automatic Data Processing Management Section, Biometry Branch, National Cancer Institute, National Institutes of Health, DHEW

Discussion of Third National Cancer Survey.

Julius Shiskin, Chief Statistician, Office of Management and Budget, Executive Office of the President

Joseph Waksberg, Associate Director for Statistical Standards and Methodology, Bureau of the Census, Department of Commerce

John J. Carroll, Assistant Commissioner for Research and Statistics, Social Security Administration, DHEW

Harold Nisselson, Assistant Director for Research, National Center for Educational Statistics, DHEW

Sigmund Schor, Director, National Center for Social Statistics, DHEW

Walt R. Simmons, Assistant Director for Research and Scientific Development, National Center for Health Statistics, DHEW

Discussion of federal statistical programs.

FIFTH MEETING, AUGUST 17-19, 1972

Alan E. Taylor, President, The Society of Certified Data Processors

Observations on the different patterns of accuracy and adequacy in automated data systems.

Harry V. Chadwick, Deputy Director, Indian Health Service, Health Services and Mental Health Administration (HSMHA), DHEW

Alfred E. Garratt, Ph.D., Chief, Office of Management Information Systems, Health Program Systems Center, Indian Health Service, HSMHA, DHEW

Rice Leach, M.D., Director, Indian Health Service Unit, Sells, Arizona

Discussion of the Indian Health Service Health Information System.

F. M. Wilkerson, Vice President for Data Services, Trans World Airlines

Discussion of the Trans World Airlines Reservation System.

Richard J. Gwin, Director General, Socio-Economic Planning, Department of Communications, Government of Canada

Discussion of Canadian perspectives on automated personal data systems and privacy.

David B. H. Martin, Special Assistant to the Secretary and Executive Director, Secretary's Advisory Committee on Automated Personal Data Systems, DHEW

Briefing on DHEW organizational structure and functions.

Inspector Donald R. Roderick, National Crime Information Center, Federal Bureau of Investigation

Special Agent Dennis Lofgren, National Crime Information Center, Federal Bureau of Investigation

Discussion of the National Crime Information Center of the FBI.

William Simmons, Director, Student Loan Program, Bureau of Higher Education, Office of Education, DHEW

Harry Lester, Branch Chief, General Education Data Systems, Division of Automated Data Processing, Office of Education, DHEW

Alice Hansen, Chief, Reports and Analysis, Division of Insured Loans, Bureau of Higher Education, Office of Education, DHEW

Carol Wennerdahl, Administrative Director, Illinois Guaranteed Loan Program

Discussion of the Guaranteed Student Loan Program.

Walter L. Schlenker, Chairman, General Electric Corporate Information Standards and Codes Committee, General Electric Company

Emmet E. DeLay, Manager, Informations Systems Operations, General Electric Credit Corporation

Discussion of individual identifiers for automated personal data systems.

Donald Roache, Acting Assistant Administrator, Program Statistics and Data Systems, Social and Rehabilitation Service, DHEW

William E. Cleaver, Senior Computer Systems Analyst, Division of State Systems Management, Social and Rehabilitation Service, DHEW

Harry Overs, Assistant Bureau Director, Bureau of District Office Operations, Division of Operating Policies and Procedures, Social Security Administration, DHEW

Richard K. M. Bridges, Assistant Director, Assistance Payments Unit, Division of Family and Children Services, Department of Human Resources, Atlanta, Georgia

Paul A. Skelton, Director, Division of Administrative Services, Department of Health and Rehabilitative Services, Tallahassee, Florida

Discussion of Social and Rehabilitation Service proposed regulations on the use of the Social Security number.

Sheila M. Smythe, Executive Associate, Blue Cross-Blue Shield, and Chairman, ANSI Committee X 3L8.3—Individual and Business Identifications

Albert C. Kocourek, Data Processing Manager, Rouse Corporation, and Chairman, Unprofessional Practices Committee, The Society of Certified Data Processors

Discussion of the proposed ANSI standard on identification of individuals for information interchange.

Paul Fisher, Chief, International Staff, Office of Research and Statistics, Social Security Administration, DHEW

Discussion of data systems for social insurance programs in foreign countries.

SIXTH MEETING, SEPTEMBER 28-30, 1972

Joseph C. Wilberding, Executive Director and General Counsel, Medical Information Bureau (M.I.B.), Greenwich, Connecticut

Discussion of the M.I.B. information system.

A. Neil Pappalardo, Vice President, Medical Information Technology, Inc., Cambridge, Massachusetts

Discussion of Meditech's medical information systems.

William F. Atchison, Director, Computer Science Center, University of Maryland, College Park, Maryland; Chairman, Education Board of the Association for Computing Machinery; and Chairman, Working Group on Secondary Education in Computers, International Federation of Information Processing Societies

Truman Botts, Executive Director, Conference Board of the Mathematical Sciences, Washington, D. C.

Peter G. Lykos, Program Director, Computer Impact on Society, National Science Foundation, Washington, D. C.

Seymour A. Papert, Professor of Mathematics and Co-Director, Artificial Intelligence Laboratory, Massachusetts Institute of Technology

Discussion of education regarding computers and their impact on society.

John N. Williamson, Ed.D., Research Specialist, The Rand Corporation, Washington, D. C.

Presentation and demonstration of REACT (Relevant Educational Applications of Computer Technology), course segment entitled "The Social Impact of Computers."

Richard T. Penn, Jr., Program Manager, Technical Analysis Division, National Bureau of Standards, Washington, D. C.

Dr. Alfred Blumstein, Director, Urban Systems Institute and Professor, Urban Systems and Operations Research, School of Urban and Public Affairs, Carnegie-Mellon University, Pittsburgh, Pennsylvania

David Storm, Assistant Vice President, First National City Bank, New York, New York

Robert R. J. Gallati, Director, New York State Identification and Intelligence System, Albany, New York

David Link, Associate Dean, Notre Dame Law School, and Chairman, Committee on Science and Technology, American Bar Association

Larry P. Polansky, Deputy Chief Court Administrator, Common Pleas Court of Philadelphia, Philadelphia, Pennsylvania

Chief Judge Harold H. Greene, Superior Court of the District of Columbia

Discussion of court record-keeping practices.

William M. Adams, Associate Director, Operations and Automation Division, American Bankers Association, Washington, D. C.

Charles Borsom, Executive Vice President, National Society of Controllers and Financial Officers, Chicago, Illinois

Richard W. Freund, Vice President, First National City Bank, New York, New York

Kenneth A. McLean, Professional Staff Member, Banking, Housing, and Urban Affairs Committee, United States Senate

Discussion of personal data systems in financial institutions.

Andrew O. Atkinson, Superintendent, Regional Computer Center, Cincinnati/Hamilton County, Ohio

William Mitchel, Senior Consultant, Claremont Graduate School, Claremont University, Claremont, California

Selma J. Mushkin, Professor of Economics, and Director, Public Services Laboratory, Georgetown University, Washington, D.C.

Charles R. Rowan, Executive Director, National Association for State Information Systems, Englewood, Colorado

Myron E. Weiner, Associate Extension Professor, Institute of Public Service, University of Connecticut, Storrs, Connecticut

Discussion of state and municipal information systems.

SEVENTH MEETING, NOVEMBER 9-11, 1972

Ralph Abascal, Managing Attorney, Law Reform Unit, San Francisco Neighborhood Legal Assistance Foundation

Discussion of the "California Earnings Clearance System."

John Shattuck, Staff Counsel, American Civil Liberties Union (ACLU)

Ira Glasser, Executive Director, New York Civil Liberties Union

Frank Donner, Research Director, ACLU Surveillance Project

Discussion of individual cases concerning automated personal data systems which have come to the attention of the ACLU.

William H. Corbett, Private Citizen

Discussion of a problem with multiple issuance of social security numbers.

Otilio Mighty, Director, Veteran's Affairs, New York Urban League

Joe Garcia, Executive Director, Seattle Veterans Action Center

Discussion of veterans' perspectives on automated personal data systems.

Gordon Manser, Associate Director, National Assembly for Social Policy and Development, Inc.

Eloise Waite, National Director for Services to Military Families, American Red Cross, and Chairman, Committee on Confidentiality of the National Assembly for Social Policy and Development, Inc.

Discussion of the National Assembly's Committee on Confidentiality and the responsibilities of voluntary social service agencies to their clients and funding sources.

Mary Drabik, Norman Matthews, and Kenneth William, People Against National Identity Cards (PANIC), Cambridge, Massachusetts

Discussion of PANIC's position on the Social Security number as a unique, universal personal identifier.

EIGHTH MEETING, DECEMBER 15-16, 1972

Robert M. Ball, Commissioner, Social Security Administration, DHEW

Discussion of policy issues raised by spread in the use of the Social Security number as a personal identifier.

NINTH MEETING, MARCH 1-3, 1973

No presentations. Meeting devoted exclusively to review of draft final report.

Other Organizations Contacted by the Committee

In September 1972, the Committee wrote to approximately 250 public interest groups and trade and professional associations seeking information about parallel studies and fact-finding efforts. Approximately 110 replied; of those, about half expressed strong interest in the Committee's work and 22 provided copies of completed studies or policy statements dealing with the handling of records about identifiable individuals. The organizations contacted by the Committee are listed below.

* American Anthropological Association
 American Association for the Advancement of Science
 American Association for Maternal and Child Health
 American Association of Retired Persons
 American Association of School Administrators
 American Association of State Colleges and Universities
 American Association of University Professors
 American Association of University Women
 American Association on Mental Deficiency
 American Bankers Association
 American Bar Association
 American Cancer Society
 American Civil Liberties Union of New York
 American Civil Liberties Union of Northern California
 American Civil Liberties Union of Oregon
 American Civil Liberties Union of Southern California
 American Civil Liberties Union of Texas
 American Collectors Association
 American College Admissions Center
 American Compensation Association
 American Correctional Association

* Sent copies of completed studies or policy statements.

American Council on Consumer Interests
 *American Council on Education
 American Dental Association
 American Economic Association
 American Federation of Government Employees
 American Federation of Information Processing Societies
 AFL-CIO
 American Federation of State, County, and Municipal Employees
 American Federation of Teachers
 American Finance Association
 American Friends Service Committee
 *American Hospital Association
 American Institute of Architects
 American Institute of Certified Public Accountants
 American Institute of Planners
 *American Institutes for Research
 American Insurance Association
 American Library Association
 American Management Association
 American Marketing Association
 American Medical Association
 American Medical Record Association
 American National Standards Institute
 American National Standards Committee 239,
 Library Work, Documentation and Related Publishing Practices
 American Newspaper Publishers Association
 *American Nurses' Association
 American Nursing Home Association
 American Personnel and Guidance Association
 American Pharmaceutical Association
 American Political Science Association
 American Psychiatric Association
 *American Psychological Association
 American Public Health Association
 American Public Welfare Association

* Sent copies of completed studies or policy statements.

American Retail Association Executives
 American School Health Association
 American Society for Industrial Security
 American Society for Information Science
 American Society for Personnel Administration
 American Society for Public Administration
 American Society of Newspaper Editors
 *American Sociological Association
 American Statistical Association (ASA)
 ASA, Southern California Chapter
 Americans for Democratic Action
 Americans for Indian Opportunity
 Associated Credit Bureaus, Inc.
 Association for Computational Linguistics
 Association for Computing Machinery
 Special Interest Group on Computers and Society
 Biomedical Computing Society
 Joint Users Group
 Association for Systems Management
 Association of American Colleges
 Association of American Law Schools
 *Association of American Medical Colleges
 Association of American Publishers
 Association of American Universities
 *Association of Computer Programmers and Analysts
 *Association of Data Processing Service Organizations
 Association of Governing Boards of Universities and Colleges
 Association of Independent Software Companies
 Association of Private Pension and Welfare Plans, Inc.
 Association of Schools of Allied Health Professions
 Association of Schools of Public Health
 Association of Social and Behavioral Scientists
 Association of Volunteer Bureaus of America
 Bank Administration Institute
 Blue Cross Association
 Brookings Institution
 Bureau of Applied Social Research, Columbia University
 Business Equipment Manufacturers Association

* Sent copies of completed studies or policy statements.

California Bankers Association
 California Rural Legal Assistance
 California State College Student Presidents Association
 California State Department of Education
 Center for Ethnic Affairs
 Center for Law and Social Policy
 Center for the Study of Democratic Institutions
 Chamber of Commerce of the United States
 *Child Welfare League of America
 Church Women United
 College Entrance Examination Board
 College Placement Council
 Committee for Public Justice
 Common Cause
 Communications Workers of America
 Community Action Council
 Computer Industry Association
 Computer Lessors Association
 *Computer Science and Engineering Board, National Academy of Sciences
 Congress on Racial Equality
 Consumer Credit Insurance Association
 Consumer Education and Protective Association
 Consumer Federation of America
 Council for Financial Aid to Education
 Council of Chief State School Officers
 Council of Graduate Schools in the United States
 Council of State Governments
 Council on Consumer Information
 Council on Social Work Education, Inc.
 Credit Research Foundation

 *Data Processing Management Association
 Daughters of the American Revolution

 Educational Development Center, The Claremont Colleges
 *Educational Testing Service

* Sent copies of completed studies or policy statements.

Family Service Association of America
 Freedom of Information Center, University of Missouri at Columbia

 Group Health Association of America, Inc.
 Guidance for Users of Integrated Data Processing Equipment

HADASSAH
 Health Insurance Association of America
 Health Insurance Institute

 Information Industry Association
 Institute for Computer Research
 Institute for Policy Studies
 Institute for Public Interest Representation, Georgetown University Law Center
 *Institute for Social Research, University of Michigan
 Institute of Criminal Law and Procedure, Georgetown University Law Center
 Institute of Electrical and Electronic Engineers
 Institute of Life Insurance
 Institute of Management Sciences
 Institute of Mathematical Statistics, Michigan State University
 Institute of Public Administration
 Institute on Law and Urban Studies
 International Association for Identification Records and Identification
 International Association of Consumer Credit Administrators
 International Association of Machine Workers
 International Brotherhood of Electrical Workers
 International Brotherhood of Teamsters, Chauffeurs, and Warehousemen of America
 International City Management Association
 International Consumer Credit Association
 International Ladies Garment Workers Union
 International Union of Electrical, Radio and Machine Workers

* Sent copies of completed studies or policy statements.

Interstate Commission on Status of Women
 Inter-University Consortium for Political Research

Joint Media Committee

*Lawyers Committee for Civil Rights Under Law
 League of United Latin American Citizens
 League of Women Voters
 *League of Women Voters (Illinois)
 Life Office Management Association

Mountain States Regional Medical Program
 Mutual Insurance Advisory Association

*National Accreditation Council for Agencies Serving the
 Blind and Visually Handicapped
 *National Assembly for Social Policy and Development, Inc.
 National Association for Advancement of Colored People
 National Association for Statewide Health and Welfare
 National Association of Broadcasters
 National Association of Consumer Credit Administrators
 National Association of Counties
 National Association of Credit Management
 National Association of Manufacturers
 National Association of Mutual Savings Banks
 National Association of Negro Business and Professional Women's
 Clubs, Inc.
 National Association of Social Workers
 National Association of State Universities and Land Grant Colleges
 National Association of Women's Deans and Counselors
 National Bureau of Standards, Institute for Applied Technology
 National Catholic Educational Association
 *National Center for Higher Education and Management Systems
 National Committee for Children and Youth
 National Committee on the Education of Migrant Children
 National Conference of Black Lawyers
 National Conference of State Social Security Administrators
 National Conference on Social Welfare

* Sent copies of completed studies or policy statements.

National Congress of American Indians
 National Congress of Parents and Teachers
 National Consumers League
 National Council of Health Care Services
 National Council of Negro Women, Inc.
 National Council of Senior Citizens
 National Council of State Education
 *National Council on Crime and Delinquency
 *National Education Association
 National Emergency Civil Liberties Committee
 National Federation of Business and Professional Women's Clubs
 National Federation of Federal Employees
 National League of Cities
 *National League for Nursing
 National Legal Aid and Defender Association
 National Municipal League
 National Opinion Research Center
 National Rehabilitation Association
 National School Boards Association
 National Small Business Association
 National Student Association
 National Student Lobby
 National Tenants Organization
 National Urban Coalition
 National Urban League
 National Welfare Rights Organization
 *Neighborhood Health Center Seminar Program (OEO)
 Neighborhood Legal Services
 New York Bar Association
 New York State Education Department
 Newspaper Guild

Ohio State Bar Association

People Against National Identity Cards
 Planned Parenthood-World Population (Planned Parenthood
 Federation of America, Inc.)
 Political Data Archive, Michigan State University
 Political Science Laboratory and Data Archive, Indiana University

* Sent copies of completed studies or policy statements.

Population Association of America
 Professional Women's Caucus
 Public Services Laboratory, Georgetown University

 Regional Social Science Data Archive, University of Iowa
 Rhode Island Consumers' Council
 Rhode Island Council of Community Services, Inc.

 Seafarers International Union of North America
 Seattle Veterans Action Center
 Sigma Delta Chi
 Simulations Councils, Inc.
 Social Data Exchange Association
 Social Science Data Archive, Survey Research Laboratory, University of Illinois
 Social Science Data Center, University of Connecticut
 Social Science Data Center, University of Pennsylvania
 Social Science Information Center, University of Pittsburgh
 Social Science User Service, Princeton University
 Society for Information Display
 Society for Personnel Administration
 Society of Data Educators
 Southern Christian Leadership Conference
 Student American Medical Association
 Student National Coordinating Committee
 Survey Research Center, University of California at Berkeley

 Travelers Aid, International Social Service of America

 United Automobile, Aircraft and Agricultural Implement Workers of America
 U.S. Conference of Mayors
 United Steel Workers of America
 Unitarian Universalist Association
 UNIVAC Users Association
 University Legal Services

 Virginia Bureau of Vital Records and Public Health Statistics

 Western Electronic Manufacturers Association
 Women's Action Alliance
 Women's Equity Action League

Appendix B

"Computers and Privacy": The Reaction in Other Countries

Common Concerns

Most of the advanced industrial nations of Western Europe and North America share concerns about the social impact of computer-based personal data systems. Although there are minor differences in the focus and intensity of their concerns, it is clear that there is nothing peculiarly American about the feeling that the struggle of individual versus computer is a fixed feature of modern life. The discussions that have taken place in most of the industrial nations revolve around themes that are familiar to American students of the problem: loss of individuality, loss of control over information, the possibility of linking data banks to create dossiers, rigid decision making by powerful, centralized bureaucracies. Even though there is little evidence that any of these adverse social effects of computer-based record keeping have occurred on a noticeable scale, they have been discussed seriously since the late sixties, and the discussions have prompted official action by many governments as well as by international organizations.

Concern about the effects of computer-based record keeping on personal privacy appears to be related to some common characteristics of life in industrialized societies. In the first place, industrial societies are urban societies. The social milieu of the village that

allowed for the exchange of personal information through face-to-face relationships has been replaced by the comparative impersonality of urban living. Industrial society also demands a much more pervasive administration of governmental activities—the collection of taxes, health insurance, social security, employment services, education—many of which collect and use personal data in an impersonal way. Nor should we overlook the increasing uniformity of industrial societies fostered by mass communications media so efficient that few issues of genuine interest and importance fail to achieve near-global extent.

Concern about the effects of computer-based record keeping appears to have deep roots in the public opinion of each country, deeper roots than could exist if the issues were manufactured and merchandised by a coterie of specialists, or reflected only the views of a self-sustaining group of professional Cassandras. The fragility of computer-based systems may account for some of the concern. It is not necessary for public opinion to be unanimously opposed to the computerization of personal-data record keeping, or even actively mistrustful of it, to destroy the effectiveness of a record-keeping operation. The active opposition of even a few percent of those whom a system means to serve can cripple the powerful, but fragile, mechanism of a highly automated system.

Nor is it necessary for this opposition to be manifested in physical sabotage of the computer itself (although that has happened); it is enough merely to withhold cooperation. There are few computer systems designed to deal with the disruption that deliberately lost or mutilated punched cards in a billing system—to give a simple example—would cause. Thus, the very vulnerability of automated personal data systems, systems without which no modern society could function, may make careful attention to the human element transcend national boundaries.

The Response in Individual Nations

WEST GERMANY

On October 7, 1970, the West German State of Hesse adopted the world's first legislative act directed specifically toward regulating automated data processing. This "Data Protection Act" applies

to the official files of the government of Hesse; wholly private files are specifically exempted from control. The Act established a Data Protection Commissioner under the authority of the State parliament whose duty it is to assure that the State's files are obtained, transmitted, and stored in such a way that they cannot be altered, examined, or destroyed by unauthorized persons. The Commissioner is also explicitly responsible for observing the effects of automated data processing on the operations of the State government, and on its decision-making powers. He must take particular note of whether computerization leads to any displacement in the *distribution* of powers among the governmental bodies of the State.

Thus, the Data Protection Act of Hesse seems designed more to protect the integrity of State data and State government than to protect the interests of the people of the State. As a pioneer statute in the field of computer law, however, its exact practical effects could scarcely have been predicted, and in no way diminish its usefulness as a guide for other jurisdictions that can learn from the Hesse experience.

To judge from the second annual report of the Data Protection Commissioner, that experience has been one of mild philosophical frustration, punctuated by occasional practical victories.¹ In one instance, the Commissioner learned of the existence of a computer in a university clinic only through a newspaper account of a fire; in another the Commissioner successfully blocked the release of criminal records to a private research center.

Based on the experience of Hesse, the States of Rheinland-Pfalz and Hamburg have passed similar acts, and the States of Baden-Württemberg, Schleswig-Holstein, Bavaria, and Lower Saxony have adopted slightly more circumscribed laws or regulations. At the Federal level, the Bundestag has considered a number of proposals for national laws of wider scope than any of the present State laws, but the estimated costs to data holders of complying with the proposed requirements for mandatory disclosure of data have thus far raised enough objections to cause the Bundestag to reconsider

¹ Federal Republic of Germany, State of Hesse, Hessischer Landtag, *Vorlage des Datenschutzauftragten* (Report of the Data Protection Commissioner), Document 7/3137, 29 March 1973. Reviewed in *Frankfurter Allgemeine Zeitung für Deutschland*, 18 April 1973; English version of review in *The German Tribune*, No. 578, 10 May 1973, p. 3.

those requirements. It seems likely, however, that some version of a relatively strong law will be passed during 1973.

SWEDEN

When strong opposition to the 1969 census erupted in Sweden, public mistrust centered not so much on the familiar features of the census itself as on the fact that, for the first time, much of the data gathering would be done in a form specifically designed to facilitate automated data processing. Impressed by the possibility that opposition might be so severe as to invalidate the entire census, the government added the task of studying the problems of computerized record keeping to the work of an official commission already studying policies with respect to the confidentiality of official records.

After a notably thorough survey of personal data holdings in both public and private systems, the commission issued a report containing draft legislation for a comprehensive statute for the regulation of computer-based personal data systems in Sweden.² The aim of the act is specifically the protection of personal privacy. Its key provisions are these:

- Establishment of an independent "Data Inspectorate," charged with the responsibility for executing and enforcing the provisions of the Data Law.
- No automated data system containing personal data may be set up without a license from the Data Inspectorate.
- Data subjects have the right to be informed about all uses made of the data about them, and no new use of the data may be made without the consent of the subject.
- Data subjects have the right of access without charge to all data about them, and if the data are found to be incorrect, incomplete, or otherwise faulty, they must either be corrected to the subject's satisfaction, or a statement of rebuttal from the subject must be filed along with the data.

² Sweden, Justice Department, *Data och integritet* (Data and Privacy), Document SOU 1972:47 (Stockholm: Almqvist & Wikström, 1972).

- The Data Inspectorate will act as ombudsman in all matters regarding automated personal data systems.

The Data Law has been passed by the Swedish Parliament and will become effective on July 1, 1973. A transition period of one year will be allowed to implement all the provisions of the law.

FRANCE

Article 9 of the French Civil Code states plainly, "Everyone has the right to have his private life respected."³ As legal scholars in all countries have noted, however, it is very difficult to define the precise limits of privacy in every case that comes before a court, and in spite of such explicit protection, the privacy of the French, both inside and outside of automated personal data systems, seems in practice no better defended than that of most other people.

Although concern about the issue of "computers and privacy" has frequently surfaced in the French press⁴ and in data-processing periodicals⁵, public interest in the subject is not deeply engaged. One bill has been introduced in Parliament, but was withdrawn pending completion of a study jointly sponsored by the Department of Justice and the Délégué à l'Informatique. An earlier study by the staff of the Conseil d'Etat seems to have influenced the proposed bill, but the legal and administrative implications of many of the features of the proposal appear never to have been carefully developed.⁶

One other development on the French scene deserves mention. The 1972 annual report of the Supreme Court of Appeals went considerably out of its way, after reviewing a case of literary invasion of privacy, to comment on the subject of computers and privacy:

³ "The Protection of Privacy," *International Social Science Journal*, XXIV, No. 3, 1972, p. 448.

⁴ *Le Monde*, November 29, 1972, pp. 20-21, for example.

⁵ *L'Informatique*, April, 1971 (entire issue).

⁶ France, Conseil d'Etat, *Rapport Annuel 1969-1970*, 3ième Parties, 2ième étude, Fascicule 3, "Les conséquences du développement de l'informatique sur les libertés publiques et privées et sur les décisions administratives," Paris, 1970.

... The progress of automation burdens society in each country with the menace of a computer which would centralize the information that each individual is obliged to furnish in the course of his life to the civil authorities, to his employer, his banker, his insurance company, to Internal Revenue, to Social Security, to the census, to university administrations, and, in addition, the data, correct or not, which is received about him by the various services of the police. When one thinks about the uses that might be made of that mass of data by the public powers, of the indiscretions of which that data might be the origin, and of the errors of which the subjects might be the victims, one becomes aware that *there* lies a very important problem, not only for the private life of everyone, but even for his very liberty.

It appears to us that this eventuality, an extremely probable one, ought to be made the object of consideration of the public power, . . . and that this consideration should take its place among the measures of precaution and of safeguard which should not lack for attention.⁷

To sum up, the situation in France is complex. The subject of computers and privacy has been given serious attention by a relatively small group of experts, but that group has an influence in government far out of proportion to its numbers. The attitude of the present government is strongly colored by another aspect of the privacy problem: It has been caught in a wiretap scandal, and its defensiveness in that regard appears to be influencing its actions on the computer front. The official report of the present working group is due before the end of 1973, but it does not seem realistic to expect that there will be any definitive action in France before, perhaps, mid-1974.

⁷ France, Cour de Cassation, *Rapport de la Cour de Cassation, Année Judiciaire 1971-1972* (Paris: La Documentation Française), 1972, p. 16.

GREAT BRITAIN

Britain is unique among the countries reviewed in having recently completed a thorough study of the entire subject of privacy.⁸ Although the committee in charge of the study, the Younger Committee, was restricted in its terms of reference to private, rather than public, organizations that might threaten privacy, the committee's report is a model of clarity and concern. In brief, the Committee found that both the customs of society and the Common law had evolved defenses against the traditional intrusions of nosey neighbors, unwelcome visitors, door-to-door salesmen, and the like. Against the new threats of technological intrusions—wiretaps, surveillance cameras, and, of course, computerized data banks—the Committee recognized that the traditional defenses are inadequate. To help deal with the threat of the computer, the Committee recommended specific safeguards to be applied to automated personal data systems, although it left the method of application up to the government to decide. The main features of the safeguards are:

1. Information should be regarded as held for a specific purpose and not to be used, without appropriate authorization, for other purposes.
2. Access to information should be confined to those authorized to have it for the purpose for which it was supplied.
3. The amount of information collected and held should be the minimum necessary for the achievement of the specified purpose.
4. In computerized systems handling information for statistical purposes, adequate provision should be made in their design and programs for separating identities from the rest of the data.
5. There should be arrangements whereby the subject could be told about the information held concerning him.

⁸ Great Britain, Home Office, *Report of the Committee on Privacy*, Rt. Hon. Kenneth Younger, Chairman (London: H. M. Stationery Office), 1972.

6. The level of security to be achieved by a system should be specified in advance by the user and should include precautions against the deliberate abuse or misuse of information.

7. A monitoring system should be provided to facilitate the detection of any violation of the security system.

8. In the design of information systems, periods should be specified beyond which the information should not be retained.

9. Data held should be accurate. There should be machinery for the correction of inaccuracy and the updating of information.

10. Care should be taken in coding value judgments.⁹

The Younger Committee also considered proposing specific legislation for automated personal data systems, based upon draft bills that had been submitted to Parliament before the Committee was formed. After concluding that the proposed laws were too constraining to be justified by the level of threat as the Committee saw it, the Committee reserved the option to recommend legislation at a later date, and confined its present recommendation to urging that the data-processing industry voluntarily adopt the safeguards as a code of good practice. This has now been accomplished in the form of a professional code adopted by the British Computer Society.¹⁰ Although only about one third of the computer professionals in Britain belong to the Society, those who do belong are, by and large, in a position to enforce the provisions of the code. Further regulation appears to be in the early stages of Parliamentary debate, and it is likely only a question of time until safeguards with the full effect of law will be in force in Britain.

CANADA

In April 1971 the Departments of Communications and Justice jointly established a Task Force on Privacy and Computers, growing out of earlier work in the Department of Communications on issues

⁹ *Ibid.*, pp. 183-184.

¹⁰ The British Computer Society, *Privacy and the Computer—Steps to Practicality* (London: The Society), 1972.

concerning the use of computers in communications. The Task Force was given broad terms of reference to consider the rights and values of the individual that cluster about the notion of privacy, and to examine present and foreseeable effects on those rights and values of computerized information systems containing personal data about identifiable individuals.

The Task Force began by carrying out a thorough survey of the status of personal data files in Canada and of the attitudes of Canadians about those files and their uses. It found that there was much more interchange of data among systems than the public realizes, that there are more inaccuracies in the files than generally realized, but that few individuals had actually experienced any intrusion on their personal privacy through either use or misuse of computers.

In its report, published in late 1972,¹¹ the Canadian Task Force concluded that computer invasion of privacy is still far short of posing a social crisis. However, the rapidly rising volume of computerized personal data and the equally rapidly rising public expectation of a right to deeper and more secure privacy threaten to converge at the crisis level. To forestall that crisis, the Task Force recommends that a commissioner or ombudsman be established in a suitable administrative setting, that carefully prepared test cases on cogent issues be brought before the courts, and that the operation of government data systems be made to serve as a national model.

¹¹ *Privacy and Computers*. A report of a Task Force established jointly by Department of Communications/Department of Justice (Ottawa: Information Canada), 1972.

REFERENCES

- British Computer Society. *Privacy and the Computer—Steps to Practicality*. London: British Computer Society, 1972.
- Canada. Department of Communication/Department of Justice. Task Force on Privacy and Computers. *Privacy and Computers*. Ottawa: Information Canada, 1972.

- Ditchley Foundation. *Private Rights and Freedom of the Individual*. Ditchley Paper No. 41. Ditchley Park, Ernstone, Oxfordshire, England: The Ditchley Foundation, 1972.
- Federal Republic of Germany. Hesse State Parliament. Data Protection Commissioner. *First Activity Report*. (Document 7/1495) 1972. *Second Activity Report*. (Document 7/3137) 1973.
- France. Conseil d'Etat. *Rapport annuel 1969-1970. Troisième partie: Réformes d'ordre législatif, réglementaire ou administratif. Deuxième étude: Les conséquences du développement de l'informatique sur les libertés publiques et privées et sur les décisions administratives*.
- Great Britain. Home Office. *Report of the Committee on Privacy*. Rt. Hon. Kenneth Younger, Chairman. London: H. M. Stationery Office, 1972.
- International Commission of Jurists. "The Protection of Privacy." *International Social Science Journal*, 24:3 (1972).
- Justice. (British Section of the International Commission of Jurists.) *Privacy and the Law*. Mark Littman and Peter Carter-Ruck, Chairmen. London: Stevens & Sons Limited, 1970.
- Lenk, Klaus. *Automated Information in Public Administration-Present Developments and Impact*. Document DAS/SPR/72.18. Paris: Organisation for Economic Co-operation and Development, 1972.
- Niblett, G. B. F. *Digital Information and the Privacy Problem*. OECD Informatics Studies, No. 2. Paris: Organisation for Economic Co-operation and Development, 1971.
- Pipe, Russell. *Data Base Developments and International Dimensions*. Document DAS/SPR/72.20. Paris: Organisation for Economic Co-operation and Development, 1972.
- Rowe, B. C., ed. *Privacy, Computers and You*. Manchester, England: The National Computing Centre Limited, 1972.
- Rule, James B. *Private Lives and Public Surveillance*. London: Allen Lane, 1973.
- Samuelsen, Erik. *Statlige databanker og personlighets vern* (Public Data-Banks and the Defense of Privacy). Oslo: Universitets Forlaget, 1972.

- Stromholm, Stig. *Right of Privacy and Rights of The Personality: A Comparative Survey*. Working paper prepared for the Nordic Conference on Privacy organized by the International Commission of Jurists, Stockholm, May 1967. Stockholm: P. A. Norstedt & Soners Förlag, 1967.
- Sweden. Justitiedepartementet. *Data och integritet* (Data and Privacy). Stockholm: Almqvist & Wiksell, 1972.
- Thomas, Uwe. *Computerized Data Banks in Public Administration*. OECD Informatics Studies, No. 1. Paris: Organisation for Economic Co-operation and Development, 1971.
- United Nations. Economic and Social Council. Commission on Human Rights. *Human Rights and Scientific and Technological Developments. Report of the Secretary-General. Addendum*. 29 December 1970.
- Warner, Malcolm, and Michael Stone. *The Data Bank Society: Organizations, Computers, and Social Freedom*. Old Woking, Surrey, England: Unwin Brothers Limited, 1970.

Appendix C

Confidentiality and the Census, 1790-1929

ROBERT C. DAVIS*

The census of population envisaged by Article I, Sec. 2 of the Constitution involved only a decennial enumeration of the inhabitants of each state, distinguishing free from slave, and excluding untaxed Indians. Yet from the beginning the census encompassed more than this minimal enumeration, and as the scope of census inquiries expanded, the confidentiality of personal data supplied for statistical purposes became an increasingly urgent issue. Gradually administrative and legal safeguards were instituted to insure confidentiality until, in 1919, it became a felony to misuse data supplied to the census by individuals. A complete study of the evolution of government policy with respect to the confidentiality of census data would necessarily involve a full-scale history of the census itself. This brief overview can at best sketch the development of that policy and indicate the major factors that appear to have shaped it.

The history of census policy on confidentiality may be conveniently divided into four broad periods. During the first six censuses (1790-1840), the confidentiality issue arose with respect to economic data. From 1850 to 1870 administrative directives extended the principal of confidentiality to all census data; with the Census

*This paper was prepared for the Secretary's Advisory Committee on Automated Personal Data Systems. It is based in part on research supported by a grant from the American Philosophical Society whose aid is gratefully acknowledged. Professor Davis is with the Department of Sociology, Case Western Reserve University.

of 1880 it became a misdemeanor to disclose information collected in the census. Thereafter, the creation of a permanent Bureau of the Census (in 1902) set in motion events that led to the Census Act of March 3, 1919, which made the unauthorized disclosure of personal data collected in the census a felony.¹

Beyond Bare Enumeration, 1790-1840

James Madison played the major role in expounding the philosophy of the first census and in establishing its procedures. Madison spoke for many of the leaders of his time when he expressed his desire to gather this "most useful information" for Congress. The census, he argued, should be "extended so as to embrace some other objects besides the bare enumeration of the inhabitants; it would enable them to adapt the public measures to the particular circumstances of the community." Echoing *The Federalist Papers*, he wished to know accurately the "several classes" of the nation so that Congress could "make proper provision for the agricultural, commercial, and manufacturing interests . . . in due proportion."²

Madison embodied his vision of the census as the vehicle for socio-economic research in a bill that divided the population into four categories: free white males, free white females, free blacks, and slaves. The free whites were to be differentiated by age—younger than 16, 16 or older—and Madison also wished to classify the population, where appropriate, under thirty occupational and industrial headings.³

¹ On the growth of the census, see: Carroll D. Wright and William C. Hunt, *The History and Growth of the United States Census*, Senate Document No. 194, 56th Congress, 1st Session, 1900, Serial 3856, and W. Stull Holt, *The Bureau of the Census: Its History, Activities and Organization* (Washington, D. C.: The Brookings Institution), 1929. See also Hyman Alterman, *Counting People: The Census in History* (New York: Harcourt, Brace & World), 1969, and Ann Herbert Scott, *Census, U.S.A.: Fact Finding for the American People, 1790-1970* (New York: Seabury Press), 1968.

² *Annals of Congress*, I, p. 1077.

³ The schedule is reproduced in Dorothy Whitson, "1970, Year of the Nineteenth Decennial Census," *Daughters of the American Revolution Magazine*, Vol. CIV (1970), p. 245.)

The Senate deleted the proposal on occupations, much to Madison's disgust, but the crucial point is that the first act pushed beyond the simple constitutional provision, thereby establishing a precedent for the enormous expansion of the census in the following century.⁴ Madison's argument for converting the census into a vehicle for statistical inquiry became the standard rationale echoed in future Congresses. In spite of occasional objections to the implied powers interpretation of Article I, Sec. 2, a Federal court was not asked to rule on the constitutionality of the expanded census until 1901. Its decision reaffirmed the necessity and right of government to gather statistics to guide public policy.⁵

Madison's statistical ideology may have looked toward the needs of an expanding nation, but his administrative conceptions with regard to the census were bound to his own time. The census bill of 1790 was based on the assumption that each enumeration was to be an *ad hoc* operation, carried out at minimal cost, and utilizing existing functionaries of government as far as possible. The bill divided the labor between the Congress, which determined the content of the census schedules, and the federal marshals, who appointed assistant marshals to do the enumeration. The thoroughness of the enumeration was to be checked by the marshals, the district courts, and the public before aggregate figures were transmitted to the national capital for compilation and publication. This system, with minor modifications, was used in the first six censuses.

Concern for accuracy is evident in the rules for enumerators. Bound by oath and threatened with fines, the assistant marshal had to file copies of his census schedules with the clerk of the district court who would make them available for inspection by the grand jury. Furthermore, the enumerator was bound to

cause a correct copy, signed by himself, of the schedule, containing the number of inhabitants, within his division, to be set up at two of the most public places within the same, there to remain for the inspection of all concerned. . . .⁶

⁴Wright and Hunt, *op. cit.*, p. 87.

⁵*U.S. v. Moriarity*, 106 Fed. 886 (C.C.S.D.N.Y. 1901).

⁶Wright and Hunt, *op. cit.*, pp. 926-927.

Both these requirements involved disclosure, but apparently the confidentiality issue was not raised. Given the few facts contained in the schedule, all of which were common knowledge locally, it is probable that most citizens did not perceive the public posting of census results as an invasion of privacy.

The practices established in the first census may have seemed sensible and frugal, but built into the procedures were a number of problems. Because data collection was decentralized, the Secretary of State had little control over the quality of the aggregate figures submitted by the marshals. The public posting of census schedules sacrificed confidentiality in the hope of attaining accuracy, a dubious proposition in the long run. And, in the absence of a permanent census bureau, expertise in the collation, analysis, and presentation of census data could not accumulate at the federal level.

The Census of 1790, published by Thomas Jefferson in the autumn of 1791, revealed a population of 3,929,214. At about the same time, Jefferson wrote to a friend that, "Making a very small allowance for omissions, which we know to have been very great, we are certainly above four millions, probably about four million one hundred thousand."⁷ Assuming that his estimate of the undercount was reasonable, one can only speculate about the causes of the difficulty.

Clearly the problems of communication and travel, especially in the frontier areas, must have been a contributing factor. Then, too, the lack of detailed instructions to the marshals must be considered. When asked to initiate the field work phase of the first enumeration, Tobias Lear, Washington's private secretary, apparently sent out copies of the census law, nothing more.⁸ The suspicion that census data would be used in levying future taxes may also have played a role in the reluctance of some citizens to cooperate.

⁷Andrew A. Lipscomb (Ed.), *The Writings of Thomas Jefferson*, Vol. VIII (Washington, D. C.: The Thomas Jefferson Memorial Association), 1905, p. 236.

⁸Tobias Lear, Circular to Marshals, March 5, 1790, in Papers of George Washington, Microfilm Edition, Series 2.

To the statistics-minded generation of the Founding Fathers,⁹ the skimpy data of the first census must have been disappointing. Jefferson's dissatisfaction is evident in the memorial regarding plans for the Census of 1800, which he sent to Congress as President of the American Philosophical Society. It called for "a more detailed view of the inhabitants," and suggested the inclusion of refined age groupings

from whence may be calculated the ordinary duration of life in these States, the chances of life for each epoch thereof, and the ratio of the increase of their population; firmly believing that the result will be sensibly different from what is presented in the tables of other countries¹⁰

The memorial suggested the age intervals that might be used, and urged that data be collected on nativity and occupation. The American Philosophical Society and the Connecticut Academy of Arts and Sciences joined forces in the advocacy of census reform, but the legislation for the approaching census showed scant evidence of their influence.

The only significant change in the schedule for 1800 was the refinement of age categories for the free white population, including females (for whom no age data were collected in 1790). The census was placed formally under the authority of the Secretary of State, but otherwise no major procedural alterations were made. Fortunately, the incumbent Secretary of State, Timothy Pickering,

⁹ Washington requested personal copies of the census returns, a move quite in keeping with his interest in the statistical study of Scotland by Sir John Sinclair. [Washington to Sinclair, March 15, 1793, in *The Correspondence of the Right Honorable Sir John Sinclair, Bart.*, Vol. II (London: H. Colburn and R. Bentley), 1831, pp. 16-17. See also Franklin Knight (Ed.), *Letters on Agriculture from His Excellency George Washington*. . . (Washington, D. C.: Franklin Knight), 1847.] Alexander Hamilton's interest in sound statistical data is shown in his research for his report on manufacturing. [Arthur H. Cole (Ed.), *Industrial and Commercial Correspondence of Alexander Hamilton Anticipating His Report on Manufacturing* (Chicago: A. W. Shaw Company), 1928.] Madison's own feelings come through in his lament to Jefferson about the truncated census bill: "It contained a schedule ascertaining the component classes of the Society, a kind of information extremely requisite to the Legislator, and much wanted for the science of Political Economy." [*Letters and Other Writings of James Madison*, Vol. I (Philadelphia, Pa.: L. B. Lippincott & Co.), 1865, p. 507.]

¹⁰ Wright and Hunt, *op. cit.*, p. 19.

was concerned about the quality of the census and drafted a set of detailed instructions to guide the marshals. He clarified the wording of the Census Act by defining terms, and he restated the categories of the census in the form of questions to be asked the head of each household. He also outlined procedures for recording, copying, posting, and aggregating the returns. On the requirement that the schedules be posted, Pickering wrote:

These copies will distinguish . . . the several families, by the names of their master, mistress, steward, overseer, or other principal person therein. The design of the copies thus set up, appears to be that if any of the inhabitants discover errors in the enumerations, they may be made known to the assistant; and the naming of the heads of families will render the detection of errors practicable.¹¹

Whether the instructions helped produce a better census is not clear, but it seems likely that it did not. The compilation of the census was placed in the hands of a State Department clerk, Jacob Wagner, and when the report appeared in 1801 its scanty data allowed little more than Jefferson's observation that "the increase of numbers during the last ten years, proceeding in a geometrical ratio, promises a duplication in a little more than twenty-two years."¹²

The third census of population merely repeated the procedures of 1800. John B. Colvin, a clerk in the State Department, issued copies of the Pickering instructions and compiled the aggregate statistics as they came in. However, the desire for economic data, voiced earlier by Madison and Jefferson, found an able advocate in the Secretary of the Treasury, Albert Gallatin. Called upon to report on the state of American manufactures, Gallatin reported to Congress the insufficient nature of such statistics and added, "Permit me to observe that the approaching census might afford the opportunity to obtain detailed and correct information on that subject"¹³ Congress immediately authorized the collection of

¹¹ Timothy Pickering, Circular to Marshals, April 30, 1800, in Pickering Papers, Massachusetts Historical Society.

¹² Lipscomb, *op. cit.*, III, p. 330.

¹³ *National Intelligencer*, April 20, 1810.

data on manufacturing establishments and their products. Gallatin drafted instructions for the enumerators in terms of broad objectives, noting that

No particular form can be prescribed, and to the request that each assistant should give in his own way the best account which, as he proceeds to take the census, he may be able to collect, I can add but very general instructions.¹⁴

The first attempt to collect economic data ended in frustration, due to the vagueness of the instructions, the carelessness of the enumerators, and the resistance of respondents. Samuel Latham Mitchill, a prominent scientist in Congress, and Tench Coxe, who had helped gather Hamilton's manufacturing data, successively worked over the material. Coxe pointed out the "numerous and very considerable imperfections and omissions" and Mitchill urged that "an exact schedule of all the subjects of inquiry ought to be formed" before the next census attempted to gather such statistics.¹⁵

In this first attempt to graft a complicated survey on a relatively simple population schedule the weakness of the early census system was bared, and the issue of confidentiality was raised for the first time. Clearly, information about business was considered a private matter by some, and it was, therefore, an issue that had to be dealt with when the fourth enumeration was planned.¹⁶

When Secretary of State John Quincy Adams confronted the problem of the Census of 1820, he set about drafting new and careful instructions. Congress had modified the census law to gather details of sex and age in the free black and slave population, but stipulated different age categories than those for free whites. As a corollary to gathering immigration data at ports of entry, the

¹⁴ *National Intelligencer*, July 2, 1810.

¹⁵ Samuel L. Mitchill, "Views of the Manufactures in the United States," *American Medical and Philosophical Register*, Vol. II (1811-1812), p. 408; and Wright and Hunt, *op. cit.*, p. 23.

¹⁶ On the problems of economic statistics, see Meyer H. Fishbein, "Early Business Statistical Operations of the Federal Government," *National Archives Accessions*, No. 54, June 1958, pp. 1-29, and "The Censuses of Manufactures, 1810-1890," *National Archives Accessions*, No. 57, June 1963, pp. 1-20.

number of foreigners not naturalized was to be ascertained, and Congress called for another attempt at gathering economic statistics. The population (including slaves) was to be classified as engaged in agriculture, commerce, or manufacturing. A supplementary act called for an enumeration of manufacturing establishments, giving details of products, their market value, and the raw materials utilized; the kind of machinery; the amount of capital invested; contingent expenses; wages and composition of the labor force. Altogether the enumeration of manufacturing establishments comprised fourteen inquiries.¹⁷

Resistance to such detailed investigations was acknowledged by treating the economic inquiry as voluntary and separate from the population schedule. Adams wrote:

as the act lays no positive injunction upon any individual to furnish information upon the situation of his property, or his private concerns, the answers to all inquiries of that character must be altogether voluntary It is to be expected that some individuals will feel reluctant to give all the information desired in relation to manufacture¹⁸

Recognition of the difficulty of obtaining "private" information of an economic nature was a beginning step toward recognition of the principle of confidentiality, but no such concept was applied to the population schedules. They were still posted "for the detection of errors which may have happened in the names of the heads of families and the numbers of persons to be returned"¹⁹

The economic data obtained by the voluntary procedure were disappointing, and objections to the economic investigation probably influenced the decision of Congress to omit such a schedule in 1830. The Census of 1830, however, did produce a significant precedent in another sector. For the first time data were collected on the blind and the deaf, a reflection of the humanitarian concern for the handicapped which was rising in America. Hesitantly, the

¹⁷ Wright and Hunt, *op. cit.*, pp. 26-27.

¹⁸ *Ibid.*, p. 136.

¹⁹ *Ibid.*

census moved toward attention to social problems that were considered outside the legislative scope of the Congress, but about which public policy was being shaped at the State level.²⁰

Insofar as centralization of records touches on the issue of confidentiality, the legislation for the 1830 census provides still another landmark. Congress provided for transmission to the Secretary of State of a copy of the schedules as well as an aggregate summary. Furthermore, the schedules of the first four censuses, preserved in the records of the district courts, were also to be sent to Washington. It appears that the impetus for this legislation was the desire to preserve the history of the nation, but it also indicated an urge for better statistical work by the Federal government, for Congress made provision for the returns of the earlier censuses to be organized and published with the results of the fifth enumeration. That products of this effort were "absolutely valueless," as a later census director put it, should not distract attention from the spirit of the legislation.²¹

A methodological advance was also recorded in the 1830 Census. Uniform printed forms were used for the first time in the enumeration, although this innovation, unfortunately, was not coupled with improvements in other fieldwork procedures. Poor fieldwork and clerical ineptitude were accompanied by the reluctance of the citizenry to answer the census inquiries. Even though economic questions were omitted, some citizens believed "that the enumeration is made with a view to the assessment of taxes, enrollment in the militia, or the collection of militia fines . . ."²²

The appetite of Congress for more and better statistics grew during the decade between the fifth and sixth censuses. A Congressional resolution calling for data on population growth and militia strength led the Department of State into an early demographic analysis to which was added a study of taxation. The debate on the tariff drew the Treasury Department into a survey of manufacturers that was more elaborate than any prior census effort. Interest also

²⁰ Harry Best, *Deafness and the Deaf in the United States* (New York: The Macmillan Company), 1943.

²¹ Wright and Hunt, *op. cit.*, pp. 28-32. Francis A. Walker's evaluation is on page 30.

²² *Hazard's Pennsylvania Register*, Vol. V (1830), p. 352.

flared briefly in a suggestion that an official statistician be appointed to make regular compilations of statistical materials useful to government, but in the end Congress fell back on the old pattern of depending on the census to carry the full burden.²³

President Martin Van Buren, responding in part to the widespread surge of statistical interest during his administration, became an advocate of a substantially enlarged Census of 1840; and Congress agreed. It acted not only to classify individuals by their economic pursuits, but to obtain

all such information in relation to mines, agriculture, commerce, manufactures, and schools, as will exhibit a full view of the pursuits, industry, education and resources of the country²⁴

Drafting the schedules was left to the Secretary of State. Accordingly, a detailed economic schedule was drawn up that probed into capital investments, forms of ownership, and output of products. The question of confidentiality was raised by these new inquiries and the instructions to the enumerators took account of it:

Objections, it has been suggested, may possibly arise on the part of some persons to give the statistical information required by the act, upon the ground of disinclination to expose their private affairs. Such, however, is not the intent nor can be the effect, of answering ingenuously the interrogatories. On statistical tables no name is inserted—the figures stand opposite no man's name; and therefore the objection can not apply. It is, moreover, inculcated upon the assistant that he consider all communications made to him in the performance of this duty, relative to the business of the people, as strictly confidential.²⁵

²³ "Statistical View of the Population of the United States from 1790 to 1830, Inclusive," *Senate Executive Document No. 505*, 23d Congress, 2d Session, 1835, Serial 252; "Documents Relating to the Manufactures in the United States," *House Document No. 308*, 22d Congress, 1st Session, 1833, Serials 222 and 223; and Frank Freidel, *Francis Lieber: Nineteenth-Century Liberal* (Baton Rouge: Louisiana State University Press), 1947, pp. 172-174.

²⁴ Wright and Hunt, *op. cit.*, p. 36.

²⁵ *Ibid.*, p. 145.

Although the economic questions were thought to merit protection, the population schedule was not. The act for the Census of 1840 retained the requirement that the results of the population count be posted in order to ascertain errors.²⁶

The detailed economic inquiries were not received with equanimity by the populace, especially in rural regions. Several counties in Virginia, Georgia, Alabama, and Louisiana refused to answer them as there was no penalty attached to noncompliance. Andrew Jackson was convinced that "the foolish questions" lost the Democrats Tennessee in the presidential election. The question in many minds, not confined to one region by any means, was voiced by a leading southern journal: "Is this federal prying into the domestic economy of the people a precursor to direct taxes?"²⁷

The defective statistics supplied by careless enumerators and evasive citizens could not be adequately detected, much less fully corrected, by the census system. William A. Weaver, who supervised the State Department clerks checking the census returns, stated that upwards of 20,000 errors were discovered in the returns from Massachusetts alone. The discovery of further errors in the printed reports led to a national discussion of census shortcomings.²⁸ Among the many voices raised, the most significant was that of the American Statistical Association. Founded in 1839, the new organization was an active critic of the official statistics on Negro insanity, data already being cited in the national controversy over slavery. As the result of its futile struggle to get corrections made in the Census of 1840, the Association became committed to the fight for a better census in 1850.²⁹

²⁶ *Ibid.*, p. 929.

²⁷ Andrew Jackson to Martin Van Buren, November 24, 1840, Papers of Martin Van Buren, Microfilm Edition; and James D. B. DeBow, *Statistical View of the United States... Being a Compendium of the Seventh Census* (Washington, D. C.: Beverley Tucker), 1854, p. 12.

²⁸ *Proceedings of the New York Historical Society for the Year 1848* (New York: The Society), 1848, p. 45.

²⁹ Albert Deutsch, "The First U.S. Census of the Insane (1840) and Its Use as Pro-Slavery Propaganda," *Bulletin of the History of Medicine*, Vol. XV (1944), pp. 469-482; Leon F. Litwack, *North of Slavery: The Negro in the Free States, 1790-1860* (Chicago: University of Chicago Press), 1961, pp. 40-46; and William Stanton, *The Leopard's Spots: Scientific Attitudes Toward Race in America, 1815-59* (Chicago, Ill.: University of Chicago Press), 1960, pp. 58-66.

The American Statistical Association was not the only source of statistical enthusiasm. In varying degrees, reform groups, business associations, medical societies and agricultural organizations expressed the need for statistics related to their specific interests. At the State and local level, statistical activities ranged from sanitary surveys to registration of vital statistics to statewide censuses of agriculture and manufacturing. A small cadre of statisticians began to grow out of this experience, but there was no central statistical bureau created in Washington to attract them to the Federal service. Unlike the situation in most European countries, statistics in the United States remained decentralized and uncoordinated.³⁰

Census Development, 1840-1880

Among all the interest groups concerning themselves with statistics there was general agreement that the Census of 1840 had been, as John Gorham Palfrey called it, "a mortifying failure,"³¹ and there was widespread agreement in Congress that the approaching Census of 1850 should be conducted in a better manner.

The statisticians of New York and Boston led the fight for census reform. In 1848 memorials from the New York Historical Society and the American Statistical Association, drafted by Archibald Russell and Lemuel Shattuck respectively, launched the effort. The burden of their advice was to start planning early and to utilize statistical experts. After much maneuvering in Congress, a bill was passed creating a Census Board to plan the schedules for the seventh enumeration. The Secretary of State, the Attorney General, and the Postmaster General constituted the Board. Rather than appoint a

³⁰ See Robert C. Davis, "The Beginnings of American Social Research," in George H. Daniels (Ed.), *Nineteenth-Century American Science: A Reappraisal* (Evanston, Ill.: Northwestern University Press), 1972, pp. 152-178; Paul J. Fitz Patrick, "Statistical Societies in the United States in the Nineteenth Century," *American Statistician*, Vol. XI (December, 1957), pp. 13-21; John Koren (Ed.), *The History of Statistics* (New York: The Macmillan Company), 1918; Franklin H. Top (Ed.), *The History of American Epidemiology* (St. Louis: C. V. Mosby), 1952; and Luther L. Bernard and Jesse Bernard, *Origins of American Sociology: The Social Science Movement in the United States* (New York: Thomas Y. Crowell Company), 1943.

³¹ *Congressional Globe*, 30th Congress, 2d Session, Vol. 18, p. 638.

statistician to commence the work, they chose instead Joseph C. G. Kennedy of Pennsylvania, whose political credentials as a fervent Whig were impeccable. Kennedy, a lawyer and journalist, soon needed expert advice, so Russell and Shattuck were called to Washington to be his statistical consultants. In spite of a complicated wrangle involving Kennedy, the Board, and the Senate census committee, a census bill emerged in May 1850. It was primarily the product of the advice of Russell and Shattuck, but Kennedy won a victory too. He was appointed to superintend the seventh census.³²

The new census schedules opened avenues of inquiry that thrust the issue of confidentiality to the fore. The schedule for the free population would list every inhabitant by name, giving, in addition, sex, age, color, nativity, place of birth, marital status, literacy, real estate ownership, and information as to whether the individual was deaf, dumb, blind, insane, idiotic, or a pauper or convict. The slave schedule was less inclusive, but more detailed than ever before. A mortality schedule listed by name all who had died in the preceding year, with personal and medical details included. The agricultural schedule covered a wide range of data on the operations of each farmer and planter; the manufacturing schedule asked for economic details on every establishment producing over \$500 annually; and the schedule on social statistics asked the enumerator to gather data on various local institutions.³³

Given the increased scope of the inquiry, the issue of confidentiality had to be faced. For the first time, the census bill did not require public posting of the population schedules, but it also made no provision for penalties for misuse of personal data. Kennedy's instructions on the point, however, were very clear.

Information has been received at this office that in some cases unnecessary exposure has been made by the assistant marshals with reference to the business and pursuits, and other facts relating to individuals, merely to gratify curiosity, or the facts applied to the private use or pecuniary

³² Davis, *op. cit.*, pp. 163-166, and Wright and Hunt, *op. cit.*, pp. 39-50.

³³ Wright and Hunt, *op. cit.*, pp. 150-153, 227-228, 234-236, 312-314, and 646-649.

advantage of the assistant, to the injury of others. Such a use of the returns was neither contemplated by the act itself nor justified by the intentions and designs of those who enacted the law. No individual employed under sanction of the Government to obtain these facts has a right to promulgate or expose them without authority.³⁴

The precise nature of the abuse of confidentiality referred to does not survive in the existing records. Although Kennedy's correspondence contains many requests for information, replies were limited to aggregate data. There is only one recorded case that might be counted as a partial exception to the rule of absolute confidentiality. A man seeking his lost brother was informed that a man of a similar name was living in Texas.³⁵ In another reply to a request for access to census schedules Kennedy wrote, "I have no objection to your taking from the office such returns as may be necessary to the purpose you name. . . ."³⁶ However, it is not possible to ascertain the nature of "the purpose" or the specific returns referred to.

When the census duties were taken over by James D. B. De Bow in 1853, the same rules of confidentiality were applied. The chief clerk of the census, in denying a request for names and personal details from the 1850 enumeration, observed that "the question is, whether it is well, in order to oblige or benefit an individual, to risk any increase of obstacles under which the Government labors in procuring such information. . . ."³⁷ De Bow felt, however, that the resistance encountered in 1840 to the economic questions had diminished. "Such objections were rarely raised in 1850," he wrote, "and in but two or three cases was it necessary to call in the services of the district attorney to enforce the requisitions of the law."³⁸

The census act of 1850 governed the Census of 1860 and Kennedy once again was appointed superintendent. The eighth enu-

³⁴ *Ibid.*, p. 150.

³⁵ J. C. G. Kennedy to S. C. Miller, November 29, 1851, National Archives, Record Group 29, Census, Item 11 (Letterbook).

³⁶ J. C. G. Kennedy to William D. Cooke, September 26, 1851, *loc. cit.*

³⁷ T. H. Baird to George C. Whiting, May 22, 1855, National Archives, Record Group 48, Department of the Interior, Office of the Secretary, Patents and Miscellaneous Division, File 183. See also Baird to Whiting, March 23, 1855, *loc. cit.*

³⁸ De Bow, *op. cit.*, p. 12.

meration had all the strengths and weaknesses of the seventh, as the schedules and procedures were fixed by law. The Civil War also put unique demands on the census: the President needed data on the probable cost of compensated emancipation; the War Department wanted quotas of draftees calculated; General Sherman needed maps showing food and forage for his March to the Sea.³⁹

It is possible that confidentiality was breached under the stress of war, but in general the work of the Census Office proceeded very much as before. The volumes on population and agriculture appeared in 1864, and the reports on manufacturing and mortality were in hand by 1865. In that year, however, Kennedy was abruptly removed from office, demonstrating once again the vulnerability of a temporary census office to the shifting fortunes of politics.⁴⁰

As the 1870 enumeration approached, it seemed evident to many statisticians that the census law of 1850 needed to be replaced with more satisfactory legislation. In Congress, the reform movement was led by James A. Garfield. After much consultation, Garfield drafted a new census act in which he sought to improve the occupational and industrial classification, to create a board to supervise the census, to shorten the census period, to improve methods of selecting census personnel, and generally to expand the number of inquiries. One suggestion had political implications. Garfield wanted to take the appointment of census enumerators out of the hands of the Federal marshals. In suggesting replacing the marshals' districts with Congressional districts as the basis for appointment of

³⁹ Typed copy of clipping, *New York Tribune*, undated, enclosed in Annie E. K. Bidwell to Walter F. Willcox, June 30, 1917, in Walter F. Willcox Papers, Library of Congress. See also General William T. Sherman, *Memoirs*, Vol. II (New York: D. Appleton and Company), 1875, p. 31; David C. Mearns (Ed.), *The Lincoln Papers*, Vol. II (Garden City, L. I.: Doubleday), 1948, pp. 587-589; and Roy P. Basler (Ed.), *The Collected Works of Abraham Lincoln*, Vol. V (New Brunswick: Rutgers University Press), 1933, pp. 160-161.

⁴⁰ James Harlan to J. C. G. Kennedy, June 2, 1865; Kennedy to Harlan, June 3 and 8, 1865; Kennedy to Andrew Johnson, June 17 and 19, 1865, in Andrew Johnson Papers, Microfilm Edition.

enumerators, Garfield was, in effect, handing the Senate's patronage to the House—a move that defeated the bill when it arrived in the Senate.⁴¹

If Garfield failed to reform the census, he succeeded in nominating its new superintendent, Francis Amasa Walker. Walker was confirmed, but he had to work within the confines of the census act of 1850 which had been modified only slightly to reflect the abolition of slavery and to eliminate some of the ambiguities in the 1850 and 1860 enumerations.⁴² Nonetheless, in his instructions to enumerators, Walker made clear his position on confidentiality:

No graver offense can be committed by assistant marshals than to divulge information acquired in the discharge of their duty. All disclosures should be treated as strictly confidential, with the exception hereafter to be noted in the case of the mortality schedule. Information will be solicited of any breach of confidence on the part of the assistant marshals. The department is determined to protect the citizen in all his rights in the present census.⁴³

The exception noted permitted the assistant marshals to submit mortality schedules to "some physician who will be willing, out of public spirit and professional interest, to glance over the entire list of diseases and correct a defective classification" of the cause of death of individuals so listed.⁴⁴

In spite of Walker's preparations, the Census of 1870 suffered from an undercount of unprecedented proportions in the South. Given the limits imposed by the act of 1850, very little could be done from Washington to prevent the fiasco. The politics of Reconstruction dictated that marshals in the South, often non-residents of

⁴¹ Mary L. Hinsdale (Ed.), *Garfield-Hinsdale Letters* (Ann Arbor: University of Michigan Press), 1949, pp. 146-147; *Congressional Globe*, 41st Congress, 2d Session, Vol. 42, Part 2, p. 1147; James P. Munroe, *A Life of Francis Amasa Walker* (New York: Henry Holt and Company), 1923, p. 109; Theodore Clarke Smith, *The Life and Letters of James Abram Garfield*, Vol. II (New Haven: Yale University Press), 1925, pp. 794-795; and Francis Amasa Walker, "American Industry and the Census," *Atlantic Monthly*, Vol. XXIV (1869), pp. 689-701; "The Census Imbroglia," *The Nation*, February 24, 1870, p. 116.

⁴² Wright and Hunt, *op. cit.*, pp. 54-56

⁴³ *Ibid.*, p. 156.

⁴⁴ *Ibid.*, p. 161.

their districts, had to appoint loyal Republicans. The liberal use of census patronage to attract freedmen to the Party led to the appointment of illiterates as enumerators. Even when the enumerators were capable people, they had to contend with white hostility and black fear. Sometimes the work was illegally subcontracted, and sometimes, as Henry Gannett reported, census data were gathered at "court sessions, musters, public meetings, etc." Walker initially estimated the undercount of Southern blacks to be about 350 to 400 thousand but he later conceded that it probably ran as high as 510,000.⁴⁵

In spite of the serious flaws in the enumeration of the South, the Census of 1870 was a marked improvement over all previous censuses. The reports were more detailed, better annotated, and the data were more clearly presented in tables and graphs. Due attention was called to limitations of the data, and Walker included a thorough historical and methodological discussion of census procedures. In a sense, the 1870 report was a brief for census reform, and that issue was joined soon again in Congress.

Census Reform, 1880-1900

Although James A. Garfield was active in promoting reform of the census, Representative Samuel S. Cox and Senator Justin Morrill led the fight in the Congress. Senator Morrill pointed out that the country had outgrown the census as conceived in 1850.

The statistical facts now required are not merely for the gratification of the curiosity of students, but are for daily, practical use in wide directions, and are to serve as the constant resource of legislators, both state and national.⁴⁶

⁴⁵ *New York Times*, March 8, 1891; Francis A. Walker, *Discussions in Economics and Statistics*, Vol. II (New York: Henry Holt and Company), 1899, pp. 49-58; and Henry Gannett, "The Alleged Census Frauds in the South," *International Review*, Vol. X (1881), pp. 459-467. The total undercount is estimated at about 1,260,000 in U. S. Bureau of the Census, *Historical Statistics of the United States, Colonial Times to 1957* (Washington, D. C.: U. S. Government Printing Office), 1960, p. 12. For the problem of underenumeration, see Advisory Committee on Problems of Census Enumeration, Carole W. Parsons (Ed.), *America's Uncounted People* (Washington, D. C.: National Academy of Sciences-National Research Council), 1972.

⁴⁶ *Congressional Record*, 45th Congress, 3d Session, Vol. 8, Part 2, p. 1049.

Representative Cox presented to the House not only an able history and critique of census practices, but also a detailed exposition of the needed reforms.⁴⁷

The 1880 census act embodied many of the reforms suggested in 1870 and added a few new provisions. Federal marshals were replaced by district supervisors as the chief local functionaries. Appointed by the President, with the advice and consent of the Senate, the district supervisors were empowered to appoint enumerators, with the consent of the Superintendent of the census. The enumerators, moreover, were to be "selected solely with reference to their fitness."⁴⁸ The topics to be enumerated were named in the act, but the Superintendent was given authority to set up the schedules and make reasonable modifications within the broad range of areas to be covered. The Superintendent was further empowered to hire "experts and special agents" to handle specific areas requiring special knowledge.⁴⁹

These reforms clearly broke with past census practices. On the issue of confidentiality, the census-taker's oath was a decisive change as well. Each enumerator now had to swear not to disclose "any information contained in the schedules, lists or statements obtained by me to any person or persons, except to my superior officers."⁵⁰ It was further stipulated that

an enumerator who shall disclose any statistics of property or business included in his return, shall be deemed guilty of a misdemeanor, and upon conviction shall forfeit a sum not exceeding five hundred dollars. . . .⁵¹

It is noteworthy that the penalty clause specifically mentions economic data, again reflecting the sensitivity felt about collecting that type of information. Notable also are the instructions to enumerators to check with attending physicians the cause of death of

⁴⁷ *Ibid.*, pp. 1534-1544, and David Lindsey, "Sunset" Cox: Irrepressible Democrat (Detroit, Mich.: Wayne State University Press), 1959, p. 190.

⁴⁸ Wright and Hunt, *Ibid.*, pp. 155-166, 936-943.

⁴⁹ *Ibid.*, p. 65.

⁵⁰ *Ibid.*, p. 937.

⁵¹ *Ibid.*, p. 938.

individuals listed in the mortality schedule,⁵² and the provision in a supplementary piece of legislation for correcting census returns by a method akin to the public posting procedure of earlier times. The enumerator was instructed to file with the county clerk a list of "names, with age, sex, and color, of all persons enumerated by him."⁵³ He was further instructed to advertise his availability for 15 days at the courthouse for the purpose of making corrections in the enumeration of population, including taking evidence under oath of needed changes, and to make known to the bystanders, if any, the outcome "of such inquiry for correction and the whole number of persons by him enumerated. . . ."⁵⁴ This availability of the facts of age, sex, and color in a semi-public setting, of course, ran counter to the growing emphasis on safeguarding the confidentiality of personal data collected by the census.

Charles W. Seaton, who, like Walker, combined political and statistical credentials, took over as Superintendent of the census in 1881. He guided the census through budget crises, fended off politically motivated charges of fraudulent counts in the South,⁵⁵ and promoted the use of mechanical aids in census work, particularly a simple tallying device that had been in limited use since 1870.

The sheer volume of data collected in 1880, especially in the area of economic statistics and special studies, was impressive. Twenty-two quarto volumes totalling 19,305 pages (plus a compendium of 1,898 pages) appeared between 1883 and 1888. Clearly, the outer limits of data management were reached in the 1880 enumeration and any further extension of the census would require a new system for data processing.⁵⁶

Herman Hollerith, a young engineer who had worked as a special agent in the 1880 Census, became interested in the problem and, after some experimentation, invented the punched card system for recording and tabulating the census returns. Hollerith's solution was as ingenious as it was simple. Hand-tallying of raw data was replaced

⁵² *Ibid.*, p. 231.

⁵³ *Ibid.*, p. 942.

⁵⁴ *Ibid.*, pp. 942-943.

⁵⁵ Gannett, *op. cit.*; Francis A. Walker, "The Eleventh Census of the United States," *Quarterly Journal of Economics*, Vol. II (1887-1888), pp. 135-161.

⁵⁶ Wright and Hunt, *op. cit.*, pp. 58-69.

by punching holes in cards whose columns corresponded to census data classifications. The cards, representing individuals or other units, were then counted electrically. Even in its earliest stage of development, the Hollerith system speeded tabulations to such an extent that its merits were demonstrable before the 1890 enumeration began.⁵⁷

The advent of the new system had dual implications for the question of confidentiality. On the one hand, it removed the actual census return one step farther from the final statistical process. On the other hand, it made possible the collection of even more information on individuals. On balance, however, it is probable that the Hollerith system enhanced the anonymity, and thus the confidentiality, of census data, although technologically it was the forerunner of modern computer-based record keeping.

The census act of 1890 followed closely the precedents set in 1880. The provisions for insuring confidentiality were similar with respect to the enumerator's oath and the penalties for unauthorized disclosure of personal data. However, the provision for depositing lists of individuals with the county courts was dropped. Instead, the Superintendent was authorized to disclose to "any municipal government," upon request, a list of names of its inhabitants, indicating "sex, age, birthplace, and color, or race." The enumerators were also instructed to check with the attending physician for the cause of death of persons reported in the mortality schedule.⁵⁸

The census reform of 1880 did not include the establishment of a continuing census bureau and the arrangements for 1890 were equally impermanent. When Robert P. Porter was appointed Superintendent, in 1889, he had to seek out former census employees, and rescue schedules and instructions from bureaucratic oblivion. The lack of continuity, the haste in organizing for the enumeration, and the problems of patronage all made Porter's position difficult. Porter's own appointment was determined more by politics than by statistical experience. A journalist-editor, he was a vigorous protectionist and served on the Tariff Commission of 1882, and had

⁵⁷ Leon F. Truesdell, *The Development of Punch Card Tabulation in the Bureau of the Census, 1890-1940* (Washington, D. C.: U.S. Government Printing Office), 1965, pp. 26-56.

⁵⁸ Wright and Hunt, *op. cit.*, pp. 233 and 948.

worked on the 1880 Census; thus, his free-trade enemies kept up a barrage of criticism until his resignation in 1893.⁵⁹ Congressional critics complained of slowness in completing the tabulations, a charge that had arisen after each previous enumeration, and threatened to close the Census Office in 1893. However, a series of enactments extended its life and placed it under the direction of Carroll D. Wright, an able statistician, who was Commissioner of Labor. The status of the census as a bureaucratic orphan brought home to many the need for a permanent Census Bureau.⁶⁰

The Census Bureau, 1902-29

The need for a continuing statistical organization was well-stated by De Bow in 1854:

Each census has taken care of itself. Every ten years some one at Washington will enter the hall of a department, appoint fifty or a hundred persons under him, who, perhaps, have never compiled a table before. . . . If any are qualified it is no merit of the system. . . . In Washington, as soon as an office acquires familiarity with statistics. . . it is disbanded, and even the best qualified employee is suffered to depart.⁶¹

In the following decades, other voices raised the same complaint, but Congress did not really begin to act seriously in the matter until the census crisis of the nineties. Then the approaching enumeration of 1900 made it necessary to organize a census office before a permanent bureau could be created. Moreover, the organization of the new office preserved an old duality in census operations, the political and the statistical. The position of Director embodied the former, while the Assistant Director was to be "a practical, experienced statistician." Political influence in census jobs was not eliminated.⁶²

⁵⁹ Holt, *op. cit.*, pp. 27-31.

⁶⁰ Wright and Hunt, *op. cit.*, pp. 69-76.

⁶¹ De Bow, *op. cit.*, p. 18.

⁶² Holt, *op. cit.*, pp. 31-34.

The act of March 6, 1902 transformed the census unit into a permanent Office, headed by a Director under whom were four chief statisticians. Provision was made for fitting census personnel into the classified civil service. The statistical duties of the office were specified and the work was spread out across the intercensal period. This is not to say that the new office settled into an uneventful period of tranquility. On the contrary, the census was to be involved in years of struggles to define its role, fend off political influence, build its professional staff, and increase the scope of its activities.⁶³

Just before the Census Office was established, a decision of the Circuit Court of the Southern District of New York gave belated sanction to the extensive work of the census. The reasoning of District Judge Edward B. Thomas was clearly Madisonian:

The functions vested in the national government authorize the obtainment of the information . . . [in order to enact] laws adapted to the needs of the vast and varied interests of the people, after acquiring detailed knowledge thereof. . . . [The government has the right to] make the researches. . . [in order to meet] its ever-widening obligations. . . to the welfare of its citizens and to the world. . . . For the national government to know something, if not everything, beyond the fact that the population of each state reaches a certain limit, is apparent, when it is considered what is the dependence of this population upon the intelligent actions of the general government.

The court then cited the wide range of social and economic problems on which Congress must legislate, and concluded that

for these or similar purposes the government needs each item of information demanded by the census act, and such information, when obtained, requires the most careful study, to the end that the fulfillment of the governmental function may be wise.⁶⁴

⁶³ *Ibid.*, pp. 34-86 (for the period 1902-1930).

⁶⁴ *U.S. v. Moriarity*, 106 Fed. 886, 891, 892 (C.C.S.D.N.Y. 1901). See 14 Am Jur 2d, Census, for an excellent summary of the legal status of the census by Henry C. Lind.

The case did not touch on the confidentiality of personal data, but confidentiality was the subject of Congressional action in the decades that followed. The act for the 1900 Census declared unauthorized disclosure of census data to be a misdemeanor punishable by a fine of up to \$500.⁶⁵ A decade later the punishment was increased: upon conviction a fine not to exceed \$1,000, or imprisonment of up to 2 years, or both, could be imposed at the discretion of the court.⁶⁶ The Act of March 3, 1919, providing for the fourteenth census, declared such disclosure to be a felony and a fine not to exceed \$1,000, or imprisonment of up to 2 years, or both, was again authorized.⁶⁷

When Congress enacted a comprehensive census law for the 1930 and subsequent censuses, it retained the penalty provision of the 1919 statute. The permanent act of June 18, 1929 also included a section that succinctly stated the safeguards for confidentiality instituted in the Bureau of the Census. Section 11 provided

That the information furnished under the provisions of this Act shall be used only for the statistical purposes for which it is supplied. No publication shall be made by the Census Office whereby the data furnished by any particular establishment or individual can be identified, nor shall the Director of the Census permit anyone other than the sworn employees of the Census Office to examine the individual reports.⁶⁸

During the same period (1900-1929), regulations about access to census records were established. Governors, municipal officers, and courts of record could obtain information from the schedules under the provisions of the various census acts. Private individuals, for "genealogical or other proper purposes," were allowed certain specific information, provided the information could not be used to the detriment of the person to whom it pertained. Free access to census data was limited to the records of the first nine enumerations.⁶⁹

⁶⁵ Act of March 3, 1899, ch. 419, sec. 21, 30 Stat. 1020.

⁶⁶ Act of March 3, 1909, ch. 2, sec. 22, 36 Stat. 8.

⁶⁷ Act of March 3, 1919, ch. 97, sec. 22, 40 Stat. 1299.

⁶⁸ Act of June 18, 1929, ch. 28, sec., 11, 46 Stat. 25.

⁶⁹ Holt, *op. cit.*, pp. 85-86.

Summary

During the first century of census activity the expansion of statistical inquiry raised the issue of confidentiality. The protection of personal data provided for statistical purposes was instituted administratively, then by statute. Before 1850, population schedules were posted publicly in an effort to detect errors, but as early as 1820 assurances of confidentiality were given for economic information. From 1850 to 1870, administrative rules extended confidentiality to all census data, but it was not until 1880 that unauthorized disclosure of information about individuals was declared to be a misdemeanor. The penalties for violating confidentiality were gradually strengthened until, in 1919, unauthorized disclosure was declared a felony.

Although it is not possible to weigh the importance of the protection of confidentiality in precise terms, it clearly seems to have been one factor that made it possible for the census to grow. Even given extensive support for the Madisonian viewpoint on the value of social statistics, the corollary guarantee of confidentiality has been needed.

As late as 1929, Herbert Hoover, in his proclamation announcing the Census of 1930, felt called upon to reassure the populace:

The sole purpose of the Census is to secure general statistical information regarding the population and resources of the country, and replies are required from individuals only to permit the compilation of such general statistics. No person can be harmed in any way by furnishing the information required. The Census has nothing to do with taxation, with military or jury service, with the compulsion of school attendance, with the regulation of immigration, or with the enforcement of any national, state, or local law or ordinance. There need be no fear that any disclosure will be made regarding any individual person or his affairs. For the due protection of the rights and interests of the persons furnishing information every employee of the Census Bureau is prohibited under heavy penalty from disclosing any information which may thus come to his knowledge.⁷⁰

⁷⁰ 46 Stat. 3012. Proclamation by Herbert Hoover, November 22, 1929.

Appendix D

The National Driver Register

DANIEL H. LUFKIN*

Scenario

Within a few hours after the hearing was over John Doe was back behind the wheel, even though the judge had suspended his license for three years. With a little planning, there's no reason for a smart fellow like Doe to be grounded for three years for reckless driving and a couple of speeding tickets, provided he takes a few simple precautions, right? As a salesman, Doe knew every county seat in the area where Colorado, Nebraska, and Wyoming join, and two days after the ticket that put him over the top in Colorado's point system, he had applied for and received driver's licenses from both Nebraska and Wyoming. The licenses were still only temporary cards, but in a week or two the real ones would be in the mail, and everything would be all right again. Of course, he'd have to be careful not to attract attention to the fact that he had an out-of-state license, but with two licenses to fall back on, Doe didn't anticipate any trouble in continuing to drive until his three years were up and he could get a Colorado permit again.

Before 1961, John Doe's plan would probably have worked. There was nothing suspicious about his looks or actions. He had

*Staff Consultant to the Committee

identified himself fully and on the application form he had answered quite truthfully that his license had never been suspended in another State. After all, the hearing at which he knew the suspension would take place was still weeks in the future when he took his precautions. Unless either Wyoming or Nebraska found something suspicious in his application, and went to considerable trouble to check with Colorado, no one would ever discover that those states were innocently, but nonetheless effectively, nullifying the judicial action of Colorado.

Today, however, any sense of smugness that Doe might feel will evaporate rapidly. The National Driver Register (NDR) of the U.S. Department of Transportation will give the motor vehicle administrations of Nebraska and Wyoming the information they need to make the proper decision about granting a license to John Doe. The mechanics of the NDR operation deserve to be developed in some detail, though needless to say, this description is by no means exhaustive: there are many bad drivers even cleverer than Doe, and they should learn about NDR the hard way. For that reason, also, the names of States used here are purely for narrative convenience; administrative and legal details do not necessarily refer to the States named.

The National Driver Register

When Doe filed his application in Wyoming, his form was processed just like all the other forms of the three hundred or so applicants that day. All were sent to the central office of the Motor Vehicle Division, where a clerk transferred to magnetic computer tape the following information from each application form: name, date of birth, place of birth, Social Security number, sex, height, weight, and color of eyes. Since Wyoming is one of the States that use the Social Security number as the driver's license number, Doe had furnished his number on the application blank. Doe's file occupied only an inch or so of tape, so Wyoming waited another week until enough applications had accumulated to fill a small reel. The reel was boxed in a metal carrier to protect the tape from stray magnetic fields that could destroy the intricate magnetic pattern of the record; then mailed to the National Driver Register at the headquarters of the National Highway Traffic Safety Administration in Washington, D.C.

In Nebraska, a slight variation of the same process was taking place. There, Doe's application was singled out early for special attention. Because the licensing system of Nebraska does not use a central computer file of all license holders, Nebraska does not routinely prepare a magnetic tape of all applicants. Instead, each local license office prepares and issues the temporary license and merely sends a duplicate record of the transaction to State headquarters. At headquarters, the record is checked against Nebraska's list of suspended drivers and, if the applicant is applying for his first license at the minimum driving age, a permanent license is issued. If the applicant is over the minimum age, however, Nebraska takes an extra precaution; it types out and forwards to the NDR a Form HS-1047 "Request for Search of National Driver Register." The information Nebraska sends about Doe is the same as the Wyoming list with one exception: Nebraska has its own system of license numbers, and does not report Doe's Social Security number to the NDR.

When the Wyoming tape reaches the NDR, it is copied onto a working tape along with all the other requests received that day. The Nebraska request for search requires one extra step. A contract data-processing service picks up all forms that are not submitted by the States in computer-readable tape or punched cards and prepares the data for the computer. This processing takes place in a facility which, like the facility at NDR itself, is protected against unauthorized access to any of the information.

When all the requests for a day's computer run have been assembled on tape, that tape, along with a master list of all drivers in the U.S. whose licenses have been reported withdrawn, is fed to the computer of the Federal Highway Administration's Computer Services Division. The two lists are matched, name for name, and all names common to both lists are printed out. The details of this process will be examined later, but for the moment, let us allow Doe his short hour of victory.

Doe's applications have reached the NDR before Colorado's report of suspension, and no match against his name appears.

Meanwhile, the case against Doe in Colorado has been going forward. His repeated offenses have earned him enough points for a three-year suspension and a heavy fine. They could also have earned him a jail sentence, but the judge noted that Doe was supporting a

family and concluded that withdrawal of Doe's driving privilege was punishment enough. The court's bailiff collected Doe's license, stamped it "Not Valid for Driving," and returned it to Doe so that he could still use it for identification when cashing checks. (Colorado even issues driver's licenses to the blind because it has become practically impossible to cash a check without one.) Some drivers in Doe's situation ruefully report to the bailiff that they seem to have mislaid their license. Although superficially attractive, this ploy is usually counterproductive, since it arouses powerful suspicion and guarantees special surveillance of the suspended driver.

In the meantime Colorado is setting out to do its part in making Doe's suspension truly effective. As soon as the court's order becomes valid, the Division of Motor Vehicles prepares an NDR Form HS-1057, "Report to National Driver Register." This report contains the same personal identification data that the search request form does and adds other information relating to the withdrawal of the license: the date of withdrawal, the date of eligibility for restoration, and a coded statement of the reason for withdrawal. The report is sent to Washington in the form of two punched cards, although other States may submit reports of withdrawal in the form of computer tape, typewritten forms, or sometimes only copies of the original court order suspending the license.

Whatever the form of entry, a report of license withdrawal is soon converted to tape format and added to the roughly 3,500,000 reports already in the master file of withdrawals that NDR maintains on 24 reels of tape. Each query from the States is compared with this master file twice; the first time within 24 hours of the time the query reaches the NDR, the second, some weeks later. It is this delayed search that is designed to outsmart the John Does who apply for a new license before their old ones have actually been withdrawn. In Doe's case, the day after the delayed search a report from NDR was mailed to both Wyoming and Nebraska, reporting that his license had been withdrawn by Colorado. Date and place of birth, Social Security or license number, sex, height, weight, and eye color were included to clinch the identification.

Verification and further action on an NDR report of license withdrawal is the sole responsibility of the States themselves, but since all States hold misrepresentation of driving record on an application

to be sufficient grounds for denying a license, both of Doe's unwitting accessories in evading the consequences of Colorado's judgment have ample reason to withdraw Doe's newly acquired licenses. Furthermore, Doe's record will stay in the master file of the NDR until a certain statutory period has elapsed. Even after his driving privilege has been legally restored by Colorado, Doe will be well advised to be completely honest in answering the question, "Has your license ever been suspended or withdrawn?"

The Withdrawal Record

Now that we have seen the NDR in operation, even if on an imaginary case, let us look at the scale of data processing and at some of the details of the searching methods. During calendar year 1972, the NDR filed just over 1,000,000 reports of license withdrawal or denial, for a daily average of over 4,000 actions. Over 17,200,000 requests for file search were received, or about 68,000 per day. About 375,000 older records were purged from the master file after their statutory applicability had expired, leaving a balance of more than 3,500,000 records valid. About three-quarters of one percent of the inquiries are identified as probably matching a record on the master file; of these, there were nearly 124,000 during the year, or about 490 per day.

Title IV of Public Law 89-563 (80 Stat. 730, 401) sets out the legal basis for the content of the master file of the NDR:

The Secretary [of Transportation] shall establish and maintain a register identifying each individual reported to him by a State, or political subdivision thereof, as an individual with respect to whom such State or political subdivision has denied, terminated, or temporarily withdrawn (except a withdrawal for less than six months based on a series of nonmoving violations) an individual's license or privilege to operate a motor vehicle.

Although the language of the law doubtless makes up in precision for what it lacks in clarity, the intent seems to be fairly plain: the NDR keeps a record of persons who have been denied a license (for inability to pass one of the required tests, for instance) or who have had their license withdrawn. The NDR reported that in 1972, 48

percent of the withdrawals were for drunken driving, 15 percent for repeated moving violations, six percent for violation of restrictions (driving during a suspension, for example), another six percent for speeding, and the remaining 25 percent for 24 miscellaneous reasons.

In reporting a denial or withdrawal to the NDR, a State must furnish at least the full name and birth year of the driver. For more positive identification, States are strongly urged to submit the full date and place of birth, an identifying number, either the Social Security number or a driver's license serial number assigned by a State, sex, height, weight, and eye color. The date of withdrawal or denial, the reason for the action, and the date on which the driver will be eligible for restoration are also reported. The reason for denial or withdrawal is reported in the standard violation code letters of the American Association of Motor Vehicle Administrators, of which the following categories are most used:

DI - Driving under influence (or impaired)	DS - Disability
FA - Fatality	FE - Felony
FR - Financial Responsibility	HR - Hit-and-run
MR - Misrepresentation	RK - Reckless
RV - Repeated Violations	SP - Speeding
VR - Violation of Restriction	

The NDR can accept the withdrawal report as a filled-in form, but it prefers, and most States supply, magnetic tape in a standardized computer-readable format.

The Request for Search

When a State wishes to have the NDR check its file for a record of an applicant, it prepares, either by hand, or as punched cards or magnetic tape, a request for search. The request must contain at least the surname and the initial of the given name and year of birth, but other identifying data, as in the withdrawal report, are usually available. As the scenario indicated, States vary in their practices in submitting these requests for search. For 1972, the NDR reported that 19 States and the District of Columbia check both original and renewal applications, 25 other States and Guam

check only original applications, while five other States, the Canal Zone and the Virgin Islands check only random samples or suspicious cases. About 80 percent of the search requests are submitted in the form of computer-readable magnetic tape.

Rescission and Restoration

If a State discovers that it has recorded a denial or withdrawal of a license by mistake, or if a person successfully appeals the action, it is the responsibility of that State to notify the NDR so that the record of the action can be purged from the files. Similarly, a State must report to the NDR that a license has been restored after the term of suspension expires. In both these cases, the NDR's search program can guarantee a match only if the report of rescission or restoration contains exactly the same data as the original report of withdrawal. States that use manual record-keeping systems sometimes cannot ensure that the two reports are exact duplicates, but States with automated systems have a number of technical methods at their disposal to generate the restoration report directly from the original, with very little chance for error. A report of rescission removes the report of withdrawal from the NDR file, but a restoration action is retained on file for the full statutory period.

The Search Process

The fundamental problem in the operation of the NDR is that of matching the *identity* of the subject of a search request with that of the subject of a withdrawal report. Although we may feel that we have an intuitive understanding of the concept of identity, there are legal and practical difficulties behind the proof of identity that greatly complicate the operation of the NDR. To begin with, most people feel that their names are the most salient features of personal identification. Although there are undoubtedly many unique names, particularly if one includes the middle name, duplicate names are far from uncommon. A study of the surnames in the files of the Social Security Administration found the following characteristics in a relatively unbiased sample of the pattern of names borne by the entire American public:

- There are more than one million different surnames in the files of the Social Security Administration, considering only the first six letters of each surname. The number of different surnames, considering the entire surname, is not estimated but is surely much higher. (The NDR files carry surnames out to a maximum of fifteen letters.)
- The ten thousand most common surnames account for only about half of the total number of Social Security accounts and account numbers.
- The two thousand most common surnames include many names most people might consider to be uncommon, such as Ham, Paris, and Mock.¹

Even though names are not by any means unique identifiers, practically every personal data system orders its files on the alphabetization of surname, first name, middle initial. Only in cases of restricted populations where the penalty for a mix-up is severe, such as customers of banks, do American filing systems depart from the pattern. (In Scandinavia, where surnames are extremely restricted, a universal identification number or other non-name identifier is a practical necessity.)

There have been several methods developed for translating a name into an unambiguous number that can serve as index to a file. The oldest of these is the Russell *Soundex* system, in which the consonants of a name are assigned numbers on the basis of a phonetic code. Since most errors in the recording of names involve mistakes in vowels or the confusion of phonetically similar consonants, the Soundex consonant numbers group easily confused consonants under the same digit (C and K, for example, or D and T, would be assigned the same number). The first letter of the surname plus the Soundex digits for the next three consonants (or zeros if there are none) form an index key that is relatively insensitive to the common errors in recording names.

¹Report of Distribution of Surnames in the Social Security Account Number File (Social Security Administration), 1964.

The Soundex system does not generate a unique number for each surname. It generates an index key under which many different (but related) surnames are grouped, usually alphabetized by first name. Thus, if Harold Baer's name happens to appear as "Harry Bayer" or "Hal Beer," the search for the proper record will have to cover a much smaller fraction of the entire surname file than if the file were arranged strictly alphabetically. In practice the Soundex code reduces the effect of spelling errors by about two-thirds.

As an alternative strategy, the file may be arranged not by name at all, but rather by an arbitrary identifying number, sometimes one furnished by the subject (such as the Social Security number) or one generated by a special computer program (such as the IBM Personal Identification Code). Computer programs are available which yield a unique number of reasonable length for the less-common surnames, but the necessity of providing tie-breaking suffixes to individualize the numbers formed from the common names can lead to key numbers of unwieldy length. It is precisely this practical problem that underlies the whole subject of record linkage and that makes the Social Security number so attractive as an identifier.²

The master files of the Social Security system itself are arranged according to the Soundex system. Persons with identical names are further identified by date and place of birth and mother's maiden name. The Social Security Administration takes special precautions in assigning account numbers to twins, triplets, etc.

The NDR search program is designed to sacrifice some efficiency for the sake of thoroughness. There, identity is sought first by surname (up to 15 letters), then by first name, then by middle name, then by date of birth. If a data element in either record (search request or master file) is blank, the program scores it as a match. To print out a possible hit requires a match on at least the surname, one initial, and two elements of the date of birth.

Thus, it is possible for *Mary Smith* born 10/12/30, to be printed out in response to a query for *Melvin Smith*, born 12/10/43, but only if there are *no* other data elements common to both records; that is, if Mary's eye color is reported but not Melvin's; Melvin's

² See E.D. Acheson, *Medical Record Linkage* (London: Oxford University Press), 1967, pp. 65-81.

height but not Mary's, etc. Along with each possible hit, the computer prints a score to evaluate the degree to which the two records match. In practice, of course, almost all record pairs have more data elements in common, and hits reported by the computer are much more closely matched than this hypothetical example.

Nevertheless, the search program is deliberately designed to be tolerant of mismatch. This is necessary because height and weight both can change, as can driver license and Social Security number. Place of birth is a strong identifier, but is susceptible to too many ambiguities (especially for persons born in metropolitan areas, where, for instance, Staten Island = Richmond Borough = New York City) to be amenable to computer processing. Thus, in spite of diligent efforts by programmers, efforts that have made the NDR name-matching program probably the best in the country, the possible hits printed out still require, and receive, careful hand-screening before they are released to the States.

This screening process is the biggest single function of the NDR staff; it employs nearly half of the organization's personnel. Of the roughly 5,000 *possible* hits produced daily, only about 500 survive human scrutiny and get passed on to the States as *probable* hits. Even so, both the NDR handbook and the "Report of Inquiry Searched," the report returned to a State, make it clear that true identity between the applicant and the individual in the master file of withdrawals and denials is only tentative. Furthermore, the file at NDR is legally only an abstract of a record that exists in the files of a State motor vehicles office. Technically, an NDR report is furnished only to help officials in one State to locate the records a driver may have established in another State.

Impact on the Public

It is difficult to disagree with the fundamental premise of the NDR: the public should be protected from irresponsible and incompetent drivers, while retaining as much jurisdictional independence as possible at the State level. But how effective is the NDR in keeping problem drivers off the roads?

Because States vary widely in their licensing practices, firm statistics are hard to find. A recent survey of Virginia's use of the NDR showed that the State had taken action against 78 percent of the

probable matches reported. Officials of Alabama estimate that they cancel about 70 licenses per month as a direct result of information supplied by the NDR. These figures extrapolated to the entire national population of licensed drivers yield an estimated 4,450 actions per month, or about 53,400 per year. Assuming an NDR budget of roughly \$1 million per year, and excluding costs incurred at the State level, this amounts to a direct cost of about \$19 per cancellation.

On the other side of the ledger, the NDR suffers from the *drag-net effect* discussed in Chapter II of this report. Before the NDR was established, States ordinarily took the time and effort to search the records of other States only when the circumstances of a license application were unusual or suspicious. Fewer applicants were caught misrepresenting their previous driving record, but even fewer innocent victims of identity mismatches were forced to prove that their driving records were, in fact, clean.

The impact of mistaken identity on innocent applicants is, of course, heavily dependent on the policy of the inquiring State. To their credit, most States do treat the NDR search report as what it is meant to be—a cautionary flag. Only one State, as a matter of policy, places the burden of proof on the flagged applicant, and even there, three-quarters of the identifications are correct. The largest group of complaints coming to the NDR's attention result from States failing to report the restoration of a license at the end of the revocation period. The NDR has no statutory authority to force individual States to comply with any minimum standard of reporting accuracy or completeness. Since a dependable, smooth-running NDR is in the best interests of all States, however, compliance is gradually improving, and as more and more States turn to automation for processing all motor vehicle records, the percentage of errors and omissions is steadily decreasing.

Of the cases of genuine mistaken identity which result in difficulty to an innocent applicant, NDR's experience is that most are so accidental that no amount of reprogramming of the computer search routines would eliminate them. Nearly all involve persons with the same names and date of birth, and with the other particulars of identification either missing from the States' reports or coincidentally identical. Recognizing that even very unlikely events occasionally happen, the NDR maintains a service representative

who contacts the appropriate State officials by telephone and acts rapidly to clear up confusion on justified complaints. Intervention by the NDR staff is required once or twice per month. Since the NDR processes about 1.4 million searches per month, NDR's contention that misidentification is a "one-in-a-million chance" seems to be borne out.

Use of the Social Security Number

From the NDR's point of view, the Social Security number is not a universal identifier, but simply one more readily obtainable element of personal identification to be used as a "tie-breaker" when more than one record in the master file has the same or similar name and date of birth as the subject of a query. Only ten States use the Social Security number as the driver license number, but that use seems to be spreading inexorably. In practice, the NDR accepts either a State license number or the Social Security number, or if special arrangements are made to alter the file format, both numbers. The NDR is aware that many people have more than one Social Security number, and that a few numbers have been erroneously assigned to more than one person, but neither of these conditions has an appreciable impact on everyday operations.

Improper Uses of NDR Data

Section 2 of Public Law 89-563, the statutory basis for NDR's operation, specifies that

Only at the request of a State, a political subdivision thereof, or a Federal department or agency, shall the Secretary furnish information contained in the register. . . and such information shall be furnished only with respect to an individual applicant for a motor vehicle operator's license or permit.

The NDR staff takes this responsibility very seriously and has designed strong protections into the data-handling process at every step of the operation. No subpoena has ever been issued for information from the master file, a fact that probably reflects two different things: first, the information contained in the master file

would not be of much use in law enforcement or in any other intelligence activity outside the driver licensing speciality; and, second, most law enforcement agencies have such good connections with the motor vehicle officials that getting a query into the NDR through regular channels would be no problem at all, provided the inquiring agency already knew enough about the suspect to insure a probable match.

Occasional requests come to the NDR from persons outside the motor-vehicle community. These are usually from persons who have misinterpreted newspaper articles about the NDR and believe that it is a master file of *all* driver's licenses ever issued, and who want to be able to prove that they once held a license and therefore should not be forced to take a road test in connection with an application for a new license. In such cases, the NDR explains its file and offers the asker the appropriate address to contact the official record keeper of the original State.

Future Developments

The present state of the NDR is the product of more than 12 years of evolution from the Register's beginnings in 1960. At first, the NDR master list was restricted to reports of withdrawals that resulted from drunken driving or culpable fatal accidents. In 1966, the law was amended to permit filing under considerably wider latitude. There are occasional suggestions from highway safety groups that the NDR become a clearinghouse for all traffic offenses, whether or not they result in the withdrawal of a driver's license. The most specific of these suggestions came from Franklin M. Kremel, President of the Automobile Manufacturers' Association of America in testimony before the Subcommittee on Roads of the House Committee on Public Works on April 12, 1972. There, Mr. Kremel proposed that "[traffic] offenses committed in any state which are subject to action in any other state go on record in the driver's home state." The same clearinghouse mechanism that the NDR now provides could accomplish such a goal, but the volume of data which would pass through such an ambitious system would require expansion of the present NDR by a factor of at least one hundred, as well as much stricter standards of driver identification than many States now use.

In connection with a scheduled rewriting of the NDR computer program to conform with new Federal standards in the programming language, the NDR has let a contract to the Safety Management Institute for a thorough study of the future need and objectives of both the States and the Federal government in the interstate exchange of driver record information to be serviced by the NDR. In particular, the contractor will examine the possibilities of operating the NDR as a shared-time system with direct-access computer terminals located at the offices of State motor vehicle authorities. (Systems of this sort are already in operation in Sweden and Great Britain where they have not only improved the control of drivers who attempt to avoid license suspension by moving from one jurisdiction to another, but also have improved the general level of service to all applicants by speeding the processing of licenses from application to issue.)

The NDR and Safeguards for Automated Personal Data Systems

The NDR is an interesting and instructive test case for the safeguards for administrative personal data systems recommended by the Secretary's Advisory Committee in Chapter IV of this report. As we have seen, the NDR is operating well in its statutory functions and although there are occasional examples of unfair treatment to individuals, these happen through circumstances beyond the control of the NDR itself, and are readily remedied through special actions of the NDR staff. Let us examine the recommended safeguards as they would apply to NDR to see whether they would forestall all unfair use of NDR data without placing a crippling burden on the system.

The first general requirement of the safeguards, *I.A.*, is that data may be transferred from a manual system into an automated system that is not protected by the safeguards only with the informed consent of the data subject. The NDR is exclusively an automated system; all its records about drivers are part of the system. Accordingly, requirement *I.A.* is not pertinent to the NDR and transfers of data therefrom.

The general personnel requirements of the safeguards, *I.B. (1)*, *(2)* and *(3)*, relate to the responsibilities of the supervisors and

employees of a system. As the foregoing description of the operation of the NDR has outlined, adherence to these requirements would be consistent with the NDR's existing operating philosophy and practices.

The requirement, *I.B. (4)*, for security precautions against unauthorized access, theft, or malicious destruction of the data is probably met to a sufficient degree, considering the anticipated threats to the system, by the security measures in force.

The restriction on transfer of data to a less secure system called for by requirement *I.B. (5)* appears to be met by present NDR practice as governed by the NDR legislation. The NDR has no statutory authority to enforce data security requirements on the licensing agencies to which it transfers data. Therefore, if the NDR has reason to doubt that any particular transferee of its data is adhering strictly to statutory limitations on the data interchange purposes of the NDR system, it can and should refrain from furnishing that agency with data.

I.B. (6) requires that a system maintain a record of access and use of the data on file. There is an internal accounting program in the NDR to record each possible match and to print out every change in the master file. The mere comparison of an inquiry against a name in the NDR does not produce a record unless there is at least a possible match.

The requirement of *I.B. (7)* that a system maintain data with appropriate accuracy, completeness, timeliness, and pertinence will present problems for intergovernmental clearinghouse systems such as the NDR and the FBI's National Crime Information Center. (The NDR is almost wholly dependent for the quality of its data base on the State agencies that furnish records of license denial and withdrawal.) Reflecting the separation of powers between the States and the Federal government, the NDR is limited under its legislation to rely on moral suasion and exhortation to convince the State agencies to conform to data quality standards for the system. The threat of expulsion from the system of a State that fails to meet NDR standards is not wholly acceptable, since the effect of excluding one State would harm other States as well. In practice, the NDR offers a program of voluntary technical assistance to help States to perfect their record-keeping systems, but it refrains from putting too much Federal pressure on politically sensitive State administra-

tions. Within the present limited scope of NDR operations, there is little risk of individuals being hurt by the quality deficiencies that may exist in the NDR State-agency-furnished data base. As we noted earlier, no actions against individuals are supposed to be taken on the basis of the reports of probable matches that are furnished by the NDR. Furthermore, the States have a collective incentive to supply accurate and timely data, because the utility of the NDR system for them depends on their doing so.

If the purposes of the system were broadened so as to require a significant increase in the scope of the NDR's data base, the difficulty of assuring data quality could increase to the point that the risk of harm to individual drivers might become substantial.

The NDR maintains a data purging schedule such as that required by *I.B. (8)*. A feature of the daily file maintenance program checks each entry for date and automatically selects those eligible for purge.

The public notice requirement of *II* should present no problem for any system; they have in principle already been met in part for the NDR through Department of Transportation booklets and press releases. Some items of information, called for in the notice requirement, which have not been publicized, could easily be added to a future publication.

Rights of individual data subjects are enumerated below as they appear in part *III* of the safeguard requirements. We summarize them for purposes of the discussion that follows:

(1) Inform an individual asked to supply data for the system whether he may legally refuse to supply the information requested.

Since the NDR system does not obtain data about individuals by requesting it from them, occasion for complying with this request would not arise for the NDR.

(2) Inform the individual, upon his request, whether he is the subject of data in the system, and, if so, make a copy available to him upon request.

The NDR could in practice comply with both elements of this requirement without difficulty provided the individual's request furnished identifying data about himself that closely corresponded to those furnished by the reporting agency in a record of his license denial or withdrawal. A search of the NDR file with mismatching query data would fail to find a record that was in the file.

As a legal and policy matter, the following points deserve mention. The NDR interprets its statute as authorizing it to provide data only to driver licensing agencies. Specific legislation might therefore be required to enable the NDR to furnish data directly to a requesting individual. (The present statute would appear not to preclude the NDR from informing an individual of the mere fact that he is, or is not, in its file.) If a request for data were made on behalf of the individual by a driver licensing agency, the NDR might properly be able to furnish the data consistent with the present statute, though it can be argued that even a licensing agency can only request an NDR report about an individual when he is an applicant for a license.

As a policy matter, it might be argued that an individual should be precluded from learning about his NDR record status on the ground that if he learned that the NDR did not have a record of some license withdrawal he had suffered, he would be free to circumvent the purpose of the NDR by making a fraudulent application, secure in the knowledge that he would not be detected. This argument might be the basis of exempting the NDR from safeguard requirement III. (2).

(3) Assure that the data are used only for the stated purposes of the system, unless the informed consent of the subject is obtained.

Adherence to this requirement by the NDR is apparently guaranteed by the strict restriction on access and use imposed by the NDR statute. That law appears to have been bent, however, in at least one instance. In a research study on the driving records of diagnosed alcoholics, the names of known alcoholics from the Maryland Psychiatric Case Register (a computer-based file of patient records from Maryland's mental-health institutions) were matched against the NDR file to determine whether clinical alcoholics had lost their

licenses for drunken driving more often than non-alcoholic drivers.³ (They had—about ten times more often.) Two points deserve to be raised in mitigation: first the purpose of the study is clearly related to the promotion of traffic safety, the fundamental purpose for which the NDR exists; second, the report of the study makes it plain that the anonymity of the subjects of both registers was carefully protected. Nevertheless, use of NDR data for research purposes is outside the authorized and stated purposes of the system.

(4) Inform the individual, upon his request, about all the uses made of the information about him, including the identity of all persons and organizations involved.

This requirement would present no technical difficulty for the NDR, since a record of all matches disseminated to the States is made as a matter of routine. The passive nature of the NDR as a clearinghouse makes it very unlikely that any match report would ever be generated which did not originate in the data subject himself making an application for a license.

(5) Assure that no data about an individual are made available from the system through compulsory legal process, unless the individual has been notified of the demand.

The managers of the NDR report that there has never yet been a subpoena issued against data in the file. This probably reflects the fact that a law-enforcement agency would have much more direct access to the same information from the original court or licensing agency records. If the police wanted to fish, however, to see whether a suspect had a license withdrawal in any State, access to the NDR system could save much time and searching. In such a case, it would be a tempting solution merely to file a bogus license application through the normal channels of query. The present law does not allow this subterfuge. An amendment proposed in 1971 (H.R. 9352, 92nd Congress, 1st Session) would have allowed the

³ Rosenberg, Nathan; Goldberg, Irving D.; Williams, George W., "Alcoholism and Drunken Driving—Evidence from Psychiatric and Driver Registers," *Quarterly Journal of Studies on Alcohol*, Vol. 33, No. 4 (December 1972), pp. 1129-1143.

NDR to furnish information to a judge upon his written request, if the information were to be used for consideration in the imposition of an appropriate sentence.

(6) Maintain procedures that allow the data subject to contest the accuracy, etc., of the data and to correct or amend faulty or controversial information.

As the NDR presently operates, once a data subject has established, through having his license application erroneously rejected, that the expiration or rescission of a prior license suspension has not been properly recorded in the NDR file, the NDR management had developed procedures for working with the appropriate State officials to correct the error in its file. (These procedures could readily be made part of the public notice statement.)

Summary

In nearly 12 years of operation, the NDR has achieved a balance between the pressures of its mission to protect the public from drivers of demonstrated incompetence or irresponsibility and the need of the public to be protected from the potential excesses of an intractable computer-based dragnet. Its operational efficiency is evident in the speed and economy with which the records are searched. Its attention to the protection of the citizens is evident in the vanishingly small number of genuine complaints that arise, and in the dispatch with which those complaints are resolved.

In the NDR, this balance has evolved through a period of time that is long in comparison to the age of many computerized systems. The procedures and safeguards developed through the experience of the NDR and other well-adapted, stable systems deserve to be widely imitated in many new systems that are still in their awkward youth or even still in gestation. The fundamental purpose of the proposed safeguards of the Secretary's Advisory Committee is to distill the qualities that make the good systems good and to apply them to all systems to forestall the growth of bad ones.

Testing the proposed safeguards against the actual conditions of operation of the NDR shows that introduction of the safeguards would by no means interfere with the work of a system of demonstrable merit. Neither would the continued operation of the NDR depend on significant deviation from the safeguards. These are clear and encouraging signs that both the NDR and the safeguards may be expected to prove durable and useful.

APPENDIX E

Computerized Criminal Information and Intelligence Systems*

The application of computer technology to criminal justice information systems was recommended by the President's Crime Commission¹ as an important tool for improving the deployment of criminal justice resources and for keeping track of criminal offenders. The commission warned, however, that special precautionary steps would have to be taken to protect individual rights and recommended that primary control of computerized information systems be retained at the state and local levels to avoid the development of a centralized file subject to Executive manipulation.

LEAA [Law Enforcement Assistance Administration, Department of Justice] has effectively concentrated a variety of resources, including research, discretionary and block grants, in the develop-

*Reprinted, with permission, from *Law and Disorder III: State and Federal Performance Under Title I of the Omnibus Crime Control and Safe Streets Act of 1968*, prepared under the direction of Sarah C. Carey for the Lawyer's Committee for Civil Rights Under Law (Washington, D.C.), 1973, Chapter II, pp. 41-49. The Acting Director of the FBI submitted comments on this paper for the record of *Hearings on Nomination of Louis Patrick Gray III*, before the Committee on the Judiciary, United States Senate, 93rd Cong., 1st Session (1973); the comments will be found at pp. 265-268 of the *Hearings*.

¹ The President's Commission on Law Enforcement and Administration of Justice. The Commission's report entitled, *The Challenge of Crime in a Free Society*, was published in February 1967.

ment of computerized information and intelligence systems. It has not, however, given adequate attention to the warnings of the Crime Commission or demonstrated adequate appreciation of the consequences of a massive accumulation of personal dossiers at the national level.

Millions of dollars of [National] Institute [of Law Enforcement and Criminal Justice] and discretionary grants have supported the creation of a national computerized file of criminal histories that is fed by LEAA block grant-funded state information systems. The initial design of the system followed the decentralized model recommended by the Crime Commission, but in January 1970, former Attorney General John N. Mitchell decided—over the objections of LEAA—to make the system a more centralized one. To accomplish this purpose, he transferred the file system from LEAA to the FBI.

LEAA has simultaneously given the states substantial grants to create intelligence systems directed primarily toward organized crime, civil disorders and the activities of dissenters. . . . Some of these files are being maintained by the same agencies that operate the more reliable information files, creating the possibility that the two will be used jointly. At the federal level the Attorney General has the power to combine intelligence with information files, but he apparently has not exercised that power, on a regular basis.

All of this has occurred without broad public policy debate about the desirability of the new systems and with little serious effort to determine whether the contribution they make to controlling crime outweighs their potential for eroding privacy and individual autonomy, or whether that potential can be reduced or controlled.

LEAA's investment in information and intelligence systems must be placed in the context of the over-all Justice Department strategy for strengthening the law enforcement capability of the federal government and for building up the powers of police and prosecutors at all levels. During his tenure as Attorney General (1968-72) John N. Mitchell made it clear that these were major goals of his administration. To this end he greatly expanded federal surveillance of citizens thought to be threats to internal security, justifying his action on the theory that the Executive has inherent and discretion-

ary power to protect itself.² He made aggressive use of existing laws, and sought and obtained significant new legislation to arm police and prosecutors with expanded authority to monitor individual conduct in order to prevent or punish potential crimes.³ These developments, when viewed in conjunction with the new surveillance technology funded by LEAA grants and the national computerized file on criminal offenders, greatly increase the capability of the government to monitor the activities of all citizens and to step in to prevent or punish those activities where it chooses to do so.⁴

The new criminal justice information network can be used in conjunction with the vast government and private computer dossiers being compiled by credit bureaus, insurance companies, welfare agencies, mental health units and others.⁵ Cumulatively, these files threaten an "information tyranny" that could lock each

² See the statement of William H. Rehnquist, *Hearings on Federal Data Banks, Computers and the Bill of Rights*, Senate Subcommittee on Constitutional Rights, 92nd Congress, 1st Session (February-March 1971) p. 597, *et seq.*, March 11, 1971. (Referred to hereafter as *Senate Constitutional Rights Subcommittee Hearings*.) The Supreme Court rejected the argument that warrantless wiretapping is permissible, in *United States v. United States District Court*, 407 U.S. 297, 40 U.S.L.W. 4761 (1972)

³ For example, under Mitchell's leadership the Justice Department implemented Titles II (expanding federal wiretapping powers) and III (weakening the strict exclusionary rules developed after the Supreme Court's ruling in *Miranda v. Arizona*) of the Safe Streets Act of 1968. In addition the department has sought and obtained new legislation such as the D.C. Crime Bill, the Organized Crime Act of 1970 and the Comprehensive Drug Abuse Prevention and Control Act of 1970, which greatly expanded federal law enforcement powers. These three bills include a number of provisions of dubious constitutionality, such as authority for preventive detention of suspects, for police to enter homes without warning ("no-knock"), for courts to impose greatly expanded sentences for "dangerous special offenders," and for grand juries to function with increased powers.

⁴ A recent federal court ruling on another matter describes the congressional intent *not* to create a national police force through the LEAA program. In *Ely v. Velde*, 451 F.2d 1131, at 1136 (4th Cir. 1972), the court stated: "The dominant concern of Congress apparently was to guard against any tendency toward federalization of local police and law enforcement agencies." Congress feared that "overbroad federal control of state law enforcement could result in the creation of an Orwellian 'federal police force' . . . The legislative history reflects the congressional purpose to shield the routine operation of local police forces from ongoing control by LEAA—a control which conceivably could turn the local police into an arm of the federal government."

⁵ The courts can and do protect individual's constitutional rights when they are specifically threatened by overt government action. But judicial intervention is, by nature, episodic and primarily remedial rather than preventive. Until governmental overreaching ripens into concrete, demonstrable injury—such as the use of illegal evidence at trial, the

citizen into his past; they signal the end of a uniquely American promise—that the individual can shed past mistakes and entanglements, and start out anew.

There are no federal and few state laws regulating the national criminal information system or its components. Few laws control the host of related public and private information systems. And any constitutional protections that exist are limited and narrowly defined.⁶ Without controls, the systems continue to evolve primarily by force of their own momentum. In part through the well-meaning actions of LEAA the prophecy of Dr. Jerome Weisner, MIT president, is being realized:

Such a depersonalizing state of affairs could occur without overt decisions, without high-level encouragement or support and totally independent of malicious intent: The great danger is that we could become information bound, because each step in the development of an information tyranny appeared to be constructive and useful.⁷

Computerized Criminal History Files

When the LEAA program began [in 1969], a few states had established centralized files of criminal offender histories to assist police departments in the identification and prosecution of suspects. For example, New York State's Identification and Intelligence System (NYSIIS), operating on an annual budget in excess of \$5 million, had more than two or three million fingerprints and 500,000 summary criminal histories on its computer.⁸ Additional

(Continued)

loss of employment or the disbanding of a political organization—the courts will not recognize that it is harmful. See, for example, *Laird v. Tatum*, 408 U.S. 1, 40 U.S.L.W. 4850 (June 26, 1972), rejecting a claim that military surveillance of persons involved in domestic political activities violates the Constitution.

⁶ In many ways these data banks are far more threatening than those maintained by criminal justice agencies. The over-all problem of computers and privacy is well presented in Miller, *Assault on Privacy: Computers, Data Banks and Dossiers* (1972), and in the hearings cited above, n.2.

⁷ *Senate Constitutional Rights Subcommittee Hearings*, March 11, 1971, p. 671.

⁸ NYSIIS performs a variety of functions in regard to this data: fingerprint processing (not yet computerized), name searching, wanted system (NCIC interface), personal appearance/arrestee file searches and review of latent fingerprinting material. (NYSIIS Fact Sheet)

fingerprints and criminal histories existed in manual files. Included in both the files were "criminal wanteds" for felonies and misdemeanors, escapees from penal institutions, parole and probation absconders, elopees from mental institutions and missing persons. More than 3,600 local law enforcement agencies submitted information to the files and used them to check out suspects and new arrests. Other states, such as California, Michigan and Florida, were developing systems, but for the most part centralized, computerized record-keeping was rudimentary. The extent to which the state files expedited or otherwise improved law enforcement had not been demonstrated.

At the national level the FBI maintained the National Crime Information Center (NCIC). This system operated through local law enforcement control terminals (as of early 1972 there were 102 terminals, of which 48 were computerized) that put the FBI in direct touch with approximately 4,000 of the nation's 40,000 local law enforcement agencies. NCIC cost about \$2.3 million per year to operate. The system contained files on stolen items, such as vehicles, firearms, boats and securities, and on wanted persons. Of the 3.1 million NCIC files, only about 300,000 were active criminal offender records. On an average, the NCIC system found a record or produced a "hit" on about 6 percent of the queries it received from local agencies (some estimates have been as low as 2 percent). In addition to the NCIC system, the FBI maintained more than 190 million identification and fingerprint files and approximately 20 million criminal offender records in permanent manual files.

Federal, state and local law enforcement agencies all contributed information to and could extract information from the NCIC files. In addition, NCIC records were searched as part of the identification service that the FBI provides for agencies of federal and state governments and other authorized institutions, including hospitals and national banks, which seek information on an individual's arrest record for purposes of employment clearances and licensing.⁹

⁹ Executive Order 10450 (April 1953) calls for an investigation of any individual appointed "in any department or agency of the government," and provides that "in no event shall the investigation include less than a national agency check (including a check of the fingerprint files of the FBI), and written inquiries to appropriate local law enforcement agencies. . . ." In *Menard v. Mitchell*, 328 F. Supp. 718 (D.D.C. 1971), the court suggested the Executive Order should be reexamined, but refused to enjoin the use

Today it is clear the NCIC and the few systems such as NYSIIS were relatively primitive, first generation data banks. In the past three years, with the investment of more than \$50 million in Institute, discretionary and block grant funds, LEAA has launched a program that by 1975 promises computerized criminal history files kept by all 50 states that will be tied in to ("interfaced with") a massive national file run by the FBI. The states will place in the central FBI file only information of public record pertaining to people who have been accused of "serious and other significant violations." The central file will consist of comprehensive histories of persons who violate federal laws or who commit crimes in more than one state and summary histories on offenders who have been involved solely in intrastate crimes.¹⁰ Any authorized inquirers¹¹ will have access to the central records, and will be referred to the relevant state files for further information. The individual state systems will include whatever information or intelligence the states choose to put into them and will be accessible on terms defined by each state.

This ambitious centralized program developed out of the System for Electronic Analysis and Retrieval of Criminal Histories (Project SEARCH), a \$16-million demonstration project supported by LEAA discretionary and Institute grants, in which 20 states shared criminal histories through a computerized central data index.¹² SEARCH was intended as a prototype for a national computer file which would facilitate prompt apprehension of interstate felons.¹³

of NCIC for this purpose. The court did preclude the distribution of arrest records except for law enforcement and federal employment purposes, but Congress overruled this exclusion in approving the FBI's 1972 appropriation (See n. 29, *infra*.)

¹⁰ Summary criminal histories contain public record information such as fingerprints (where available), personal description, arrests, charges, dates and places of arrest, arresting agencies, court dispositions, sentences, limited institutional data and limited information concerning parole and probation.

¹¹ "Authorized inquirers" include any agency that now participates in the FBI's system, plus any agency subsequently permitted to do so by the Attorney General.

¹² The states participating in the SEARCH experiment were Arkansas, Arizona, California, Colorado, Connecticut, Florida, Georgia, Illinois, Maryland, Massachusetts, Michigan, Minnesota, Nebraska, New Jersey, New York, Ohio, Pennsylvania, Texas, Utah and Washington.

¹³ As the FBI put it: "The purpose of centralization. . . is to contend with increasing criminal mobility. (NCIC Advisory Board, "Computerized History Program: Background,

(Continued)

The project was funded through the California Council on Criminal Justice. Primary developmental responsibility was contracted to Public Systems Inc. (PSI), a research and development firm based in San Jose.¹⁴ PSI was aided by task forces and advisory committees composed of representatives from the participating states. The major assignment of the SEARCH group was to develop standard, computerized criminal history records, summaries of which could be filed in a central index. Computer terminals in the individual states could submit information to the central index and query it for identification of suspects. If the central index contained matching references concerning the subject of a query, the summary index data was transmitted to the inquiring police officer and he was told which state had the full file on the suspect. The officer could then request and obtain a copy of the suspect's full record via teletype from the state agency. The initial focus of the system—like its predecessors—was on police requirements; but the project design anticipated subsequent development of a capability to service the information needs of courts and corrections officials as well.¹⁵

On March 9, 1971, LEAA Associate Administrator Richard W. Velde testified before the Senate Subcommittee on Constitutional Rights that:

The basic problems facing SEARCH in the demonstration period have been solved. A common format for criminal histories was developed, and in machine-readable form. Each

(Continued)

Concept and Policy," as approved March 31, 1971, and amended Aug. 31, 1971.) FBI data show that 25 percent of arrests involve interstate movement by felons. A preliminary survey by SEARCH put the figure at around 27 percent but estimated that most of these arrests were in contiguous states.

¹⁴ Eight of PSI's key personnel are from Sylvania Sociosystems Lab (a research and development arm of GTE Sylvania), and one is the former head of California's SPA, the California Council on Criminal Justice.

¹⁵ We disagree with LEAA's assumption that across-the-board increases in offender data are desirable for all decision-making processes within the criminal justice system. For example, arrest records not followed by convictions or juvenile offenses probably should not be made available to sentencing judges or to parole boards. LEAA recently made a grant to the Federal Judicial Center to finance the transfer of all data processed through the Federal courts to the Justice Department. Sen. Ervin has questioned the propriety of this arrangement under the separation of powers principle. (Letter of July 27, 1972, from Sen. Ervin to the Hon. Alfred P. Murrah, Federal Judicial Center.)

active participant converted at least 10,000 felony records to the SEARCH system for the demonstration. As the test period showed, a state making an inquiry of the central index with perhaps no more information than a driver's license number could find out if that person were in the (national) index and then be switched to the state holding the complete criminal history. It takes merely seconds to do all of that and receive the information.¹⁶

Computer experts were less sanguine about the success of the experiment. Some noted that only a small number of the SEARCH states had actually participated in the demonstration and suggested that the test simply duplicated what the FBI's NCIC had already demonstrated. *Datamation* magazine reported on the SEARCH demonstration as follows:

Ten states officially participated in the demonstration, but only New York made any extensive operational uses of the system, and a total of only five states conducted any demonstrations. . . . SEARCH met its demonstration objectives from a conceptual point of view, but did not achieve much operational success, because of design compromises, lack of updating capability for the central index and failure to develop record formats acceptable to all users, among other reasons.¹⁷

Despite these criticisms, and over the protests of LEAA Director Jerris Leonard and the states that had participated in the project, SEARCH became the launching pad for an expanded and "improved" criminal offender system to be operated by the FBI. Transfer of system control to the FBI meant that, instead of a network of state-controlled files tied into a limited central index, the SEARCH system became a national file run by a line operating agency. More importantly, judging from the debate on the subject that raged for months, FBI control meant diminished operational standards for the system's integrity, and attenuation of safeguards for individual privacy.

¹⁶ *Senate Constitutional Rights Subcommittee Hearings*, p. 611.

¹⁷ Phil Hirsch, *Datamation* magazine, June 15, 1971, pp. 28-31.

The conflict between the FBI and the Project SEARCH group had emerged in May 1970. In a letter dated May 8, 1970, Jerome J. Daunt, then director of the FBI's NCIC system, wrote to the SEARCH group complaining about various recommendations in the Interim Report of the SEARCH Committee on Security and Privacy. Among other items, the letter stated:

Throughout the report Project SEARCH is described as an ongoing system. Future developments of this system are not the proper objectives of the Project SEARCH group. . . .

In view of the limited purpose of the Project SEARCH, further studies in the area of privacy and security are not justified. If there is a need, it should be done by some other body.

The conflict became more pointed. In a letter of Oct. 15, 1970, John F.X. Irving, then chairman of the state planning agency's executive committee, wrote to Attorney General Mitchell protesting the proposed transfer of control over the SEARCH system to the FBI as well as certain "changes in direction" of the system. Irving complained that duplication would result because the states intended to continue developing their own system¹⁸ and protested that the FBI's plan to focus on data useful to the police only ignored the needs of courts and corrections agencies. Irving also argued that the FBI system, by dealing directly with city police departments instead of going through the states, would subvert the federal-state relationship contemplated by the Safe Streets Act.

The strongest protest in Irving's letter was directed to the potential invasions of privacy inherent in a federal information system.

Last, but certainly not least, the FBI's proposed file is significantly different in both conception and content from the state-held files contemplated by Project SEARCH. The basic underlying concept of Project SEARCH is that no new national data banks or criminal history files should be created

¹⁸ By altering the basic system design for SEARCH, FBI requirements could increase the cost by 30 to 40 percent, apart from the possible duplication involved. Interview with Jerry Emmer, LEAA official.

because of the inherent threats to individual privacy and the security of records. The Project SEARCH operating concept is state-held files with a national index or directory of offenders. . . . The FBI file, on the other hand, would contain as much detailed data on offenders as the FBI was willing and able to collect. It is not a true index but rather a federal data bank on offenders.

The FBI countered that expanding SEARCH as a state-dominated system would increase the over-all costs and would duplicate the NCIC system. More importantly, a system subject to the control of 50 state executives could be abused too easily. As Jerome Daunt put it: "If the governor controlled the system, he could control who gets elected."

The protests by the states and by Jerris Leonard were to no avail. The FBI took control of the SEARCH index in December 1970. The decision was John Mitchell's. In November 1971 the bureau notified the press that:

The Federal of Investigation has begun operation of a computerized criminal history data bank that eventually will give police almost instantaneous access to an individual's criminal arrest record from all 50 states and some federal investigative agencies and the courts. . . . The system. . . will make available by 1975 on a nationwide computer network most of the information now handled through the FBI's vast criminal record and fingerprint files. . . . It replaces a pilot effort, called Project SEARCH, in which only a computerized index was maintained, capable of telling police if a suspect had a record.¹⁹

Although the November 1971 announcement signaled the end of LEAA control of the system, the agency has continued to be involved in the development and expansion of information systems. Project SEARCH has been given discretionary and research grants for developing related technology, such as satellite transmission of information, automatic fingerprint identification/verification and additional work on transaction-based criminal justice statistics. And

¹⁹ Justice Department news release, November 1971.

LEAA block grants have continued to serve as the primary source of funding for the state information systems that will be the major components of the NCIC criminal history information system. Despite LEAA's expressed concern for privacy considerations in the operation of information systems, it has not sought to precondition the use of its funds for such systems on the development by the states of adequate statutory or regulatory safeguards.

It is difficult to obtain reliable information concerning the present or projected scope, cost or structure of the new FBI data bank. At the federal level a variety of agencies are scheduled to participate in the system, most of which have been previously active in the NCIC system. Among others, the system will receive data and answer inquiries from the Secret Service, the Internal Revenue Service, the Alcohol and Tax Division of the Treasury Department, the Bureau of Customs, the Immigration and Naturalization Service, the Bureau of Prisons, the U. S. Attorneys and U. S. Marshals. As far as the states are concerned, at the time of the FBI's November 1971 press release, only one state—Florida—was actually contributing information to the file. The next two states—New York and California—were not scheduled to participate until July 1972. (. . . California will probably not be ready for full participation until 1973.) In most instances, the states do not have their own systems operational—or even designed.

Official estimates of the total number of individuals who will eventually be included in the national file range from five million (the FBI estimate) to 20 million or more (the LEAA estimate). The number of files in the total system including all the state files will, of course, be much greater. Neither LEAA nor the FBI will provide information on the total costs involved.

Nor is it clear whether the FBI's file will be comprehensive, or simply a summary index that refers inquirers to the state files. The FBI has stated that it plans to maintain complete files only on offenders who have been arrested in more than one state, maintaining "summary files" on offenders who have been arrested within a single state only. State control centers will be able to add or remove information from the national file. However, for those states that have not yet built a central computerized information file, the FBI is presently maintaining complete offender files in both situations. The fact that the agency is presently maintaining

complete files for all states makes is doubtful that they will subsequently abandon those files.²⁰

The kinds of information to be stored in the data file and the conditions of participation in the system are not defined by statute or by formal regulations. The only standards regulating the system are those set forth in the NCIC Advisory Board policy paper.²¹ Each state seeking to participate in the system must sign a contract with the director of the FBI, agreeing to abide by the terms of the policy paper and by any "rules, policies and procedures hereinafter adopted by NCIC." The contracting state must also agree to indemnify the federal agency against any legal claims arising out of the operation of the information system. The FBI claims that the majority of the states—"all but three or four," according to Daunt, "and those have technical not substantive problems with the system"—have signed the contract and thereby accepted the terms of the policy paper.

The NCIC standards are substantially less rigorous than those developed by LEAA's Project SEARCH, and in many instances their adoption was met by vigorous objections from LEAA, the SPAs [state planning agencies] and the Project SEARCH participants.

Under the NCIC policies, the national file is restricted to data on "serious and other significant violations." This is defined by exclusion:

Excluded from the national index will be juvenile offenders as defined by state law (unless the juvenile is tried in court as

²⁰ The basic policies developed for the FBI system by the NCIC Advisory Policy Board state:

In the developed system, single state records will become an abbreviated criminal history record in the national index with switching capability for the states to obtain the detailed record. Such an abbreviated record should contain sufficient data to satisfy most inquiry needs, i.e., identification segment, originating agency, charge data, disposition of each criterion offense and current status. This will substantially reduce storage costs and eliminate additional duplication.

²¹ The NCIC Policy Paper, *supra* n. 13. The board is appointed by and serves at the discretion of the director of the FBI. Its members are individuals responsible for the administration of state information systems or state or local terminals on the NCIC system. Recently, procedures were introduced for electing board members from among participating state officials. It does not include constitutional lawyers, computer experts or other nonlaw enforcement representatives.

an adult); charges of drunkenness and/or vagrancy; certain public order offenses, i.e., disturbing the peace, curfew violations, loitering, false fire alarm; traffic violations (except data will be stored on arrests for man-slaughter, driving under the influence of drugs or alcohol, and "hit and run"); and non-specific charges of suspicion or investigation.²²

Narcotic or mental commitment records will be maintained if they are part of the criminal justice process. Domestic crimes such as nonsupport or adultery and victimless crimes such as homosexuality, gambling and others are considered "serious" in some jurisdictions.²³ Moreover, any state or locality may store additional information in its own files, which can be disseminated upon requests referred to the state or local police department by the central index.²⁴ Besides the criminal record data on serious offenders, the Justice Department has asserted an absolute right to keep records on persons who are "violence prone" and other "persons of interest" for national security reasons.

Contributions to each individual file depend on participating state and local agencies. According to the NCIC policy paper, each file is supposed to show arrests, charges, the disposition of each case, sentencing details and custody and supervision status, but experience indicates that agencies contributing to the files rarely remove arrests records that do not lead to convictions²⁵ and often

²² NCIC Policy Paper, *supra* n. 18 p. 11.

²³ HR 1, the welfare reform proposal which was extensively revised by the Senate Finance Committee before the 92nd Congress adjourned, would make nonsupport a federal crime and place a special assistant U.S. attorney in every judicial district to prosecute violators whose desertion caused their families to go on welfare. This new crime would assure that personal data files on welfare recipients will be mingled with the files on criminal offenders.

²⁴ A number of jurisdictions maintain harmful, irrelevant data. The Kansas City, Mo., ALERT System, for example, includes the following categories of information in its computerized Warrant/Want Real Time Files: "local and national intelligence on parole status; active adult and juvenile arrest records with abstract data, area dignitaries; persons with a history of mental disturbance; persons known to have confronted or opposed law enforcement personnel in the performance of their duty; college students known to have participated in disturbances primarily on college campus areas." (Statement of Sen. Charles Mathias, March 9, 1971, *Senate Constitutional Rights Subcommittee Hearings*, p. 576.)

²⁵ The inclusion of arrest records that do not lead to conviction is particularly onerous. In 20 to 30 percent of arrests, the police do not bring charges for a variety of reasons

include damaging extenuating information. Personal identification information such as name, age, sex and physical description are included as well as FBI numbers, state numbers, social security numbers, date and place of birth and other miscellaneous numbers. At least one criminal fingerprint card is filed in the FBI identification division "to support the computerized criminal history record in the national index."²⁶

No federal law or regulation calls for deletion of outdated records. The NCIC policy paper states: "Each control terminal agency shall follow the law or practice of the state. . .with respect to purging/expunging of data entered by that agency in the nationally stored data" (p. 12). Most states have no purging requirements at present. The policy paper endorses the concept of state and federal penalties for misuse of the data,²⁷ and suggests that the individual be given the right to see and correct his file, but makes no specific recommendations. Experience at the state and local levels indicates that it is extremely difficult for an individual to correct an erroneous or incomplete file without resorting to lengthy court proceedings.

The major deficiency in the guidelines and the system as a whole is the absence of proper controls on access to the data contained in the files. The policy paper states that access will be provided primarily to criminal justice agencies in the discharge of their official responsibilities. In addition, "agencies at all governmental levels which have as a principal function the collection and provision of fingerprint identification information" will have access, as will all those agencies that presently use NCIC. This means that the files will still be used for clearing Federal employees and the

including mistaken identification, lack of evidence, etc. Yet only eight states have statutes providing for expungement of such records. And of the eight, only one allows expungement of arrest records for an individual who has had a previous conviction.

²⁶ NCIC Policy Paper, *supra* n. 13.

²⁷ At present the only penalty for misuse of data maintained in the NCIC system is the provision in 28 USC §534 allowing the FBI to withdraw the privilege of participating in the exchange system from an agency that fails to abide by NCIC standards. As the exercise of that sanction means that the agency would also cease contributing data to NCIC, the provision has been invoked rarely. 18 USC §1905 provides weak criminal sanctions for the disclosure of confidential financial information by federal officials. It would not extend to the state participants in the NCIC system, and it protects only white-collar criminals whose offenses involve financial misdealings.

employees of Federal contractors,²⁸ and the information will be shared with federally insured banks, hospitals, insurance companies, etc.²⁹

At the stage level, the NYSIIS experience suggests that a wide range of state agencies and some private firms will have access to the files for clearing potential employees or licensees.³⁰ The guidelines provide that state agencies (except for criminal justice agencies) cannot use the data in connection with licensing or state and local employment, unless "legislative action at the state and federal level or Attorney General Regulations" provide otherwise. But, as the New York experience shows, a number of states already have clearance authorization laws, and, since Congress has authorized the sharing of identification information with such states—with the approval of the Attorney General—the exclusion promises to be of limited value. (The Attorney General has never withheld approval from a state agency seeking access.) Even if approval or clearance should be denied, local policy will inevitably determine the terms of access because the NCIC system lacks adequate sanctions to apply to nonconforming states. At least one state, Iowa, is considering making the information available to anyone willing to pay for it.³¹

²⁸ Federal contractors such as Lockheed Aircraft have in the past obtained such records from the federal departments with which they do business.

²⁹ On Dec. 3, 1971, Congress approved, as part of the fiscal 1972 FBI appropriation, the following blanket authorization for the distribution of FBI data:

The funds provided in the Department of Justice Appropriations Act, 1972 for Salaries and Expenses, Federal Bureau of Investigation, may be used, in addition to those uses authorized thereunder, for the exchange of identification records with officials of federally chartered or insured banking institutions to promote or maintain the security of those institutions, and, if authorized by state statute and approved by the Attorney General, to officials of state and local governments for purposes of employment and licensing, any such exchange to be made only for the official use of any such official and subject to the same restriction with respect to dissemination as that provided for under the aforementioned Act. (*Congressional Record*, Dec. 3, 1971, S 20461.)

In 1972 a proposal was submitted to Congress to reverse the 1971 action. At the time of this report that proposal, an amendment to the pending Justice Department appropriation bill, was before a House-Senate Conference Committee. In the meantime the Justice Department (through Sen. Hruska) introduced S 3834 (HR 15929) to assure the broad availability of FBI records.

³⁰ See letter from Aryeh Neier, executive director of the American Civil Liberties Union, to Sen. Sam J. Ervin (D-N.C.), March 23, 1971 (copy on file with the Senate Subcommittee on Constitutional Rights), listing state agencies with access to NYSIIS files.

³¹ *Des Moines Sunday Register*, July 2, 1972, p. 3A.

The looseness of the access provisions becomes more ominous in view of the parallel rapid growth of law enforcement intelligence files containing sensitive and unsubstantiated information.³² In addition, the provisions virtually invite linkages with information files maintained by public and private agencies. LEAA is presently cooperating with HUD and several other federal agencies to fund experimental programs in six cities³³ that will provide city managers or mayors with "integrated municipal information systems" (IMIS) for management purposes. The IMIS is being promoted by the National League of Cities as a "significantly new approach to the process of local government itself," one "that will require a degree of commitment and level of expenditure by municipalities which has never before been associated with computer-based systems." The new systems will eventually include data from all urban service departments—police, welfare, schools, etc.—as well as underlying demographic and other facts that could be useful in making urban management decisions. The enlarged, organized data base supposedly will point to new relationships among urban problems, and consequently will improve policy-making.

The IMIS could present serious problems. . . . As Robert Knisely, the director of the program, has written:

If vital statistics, and school, employment and criminal justice records can be pulled together on a named individual at will, a child's teachers may find out he is illegitimate, his poor grades may keep him from getting a job, his lack of a job may

³² We have already pointed out that LEAA is funding regional and state intelligence networks for the collection and analysis of data on organized crime, as well as state and local intelligence-gathering systems on civil disorders and militants and other nonconformers. Because of the difficulty of standardizing intelligence information, it is unlikely that interstate computer exchange of such data will be realized, at least for some time. However, once the data are centralized at the state level under the auspices of the agency responsible for operating the central criminal information files, it becomes accessible to other state or federal agencies who will be directed to the state of record through the NCIC system. And the Attorney General has the power under the present statutory scheme to combine federal investigative and intelligence files with the NCIC criminal offender files.

³³ The IMIS cities are: Dayton, St. Paul, Long Beach, Calif., Reading, Pa., Charlotte, N.C., and Wichita Falls, Tex. Other jurisdictions are combining criminal justice computer data with information from other public agencies on their own.

lead to crime and his criminal justice records may keep him permanently unemployed.³⁴

Although Knisely sees certain potential benefits in the program, he concludes that they are overbalanced by the likelihood that neither the courts nor the legislatures will exert adequate control over the emerging technology. In any event, the possibility that criminal information files will become a part of a larger citywide integrated information system is a real one. In California, Iowa and other jurisdictions, data from a variety of social service agencies are already being combined in a single administrative unit that is also responsible for criminal justice data.³⁵

Beyond IMIS, which is a deliberate, small-scale experiment, it is likely that private and public decision-makers will step up their generalized demands for whatever data are available on the individuals with whom they are concerned.³⁶ Senator Sam Ervin (D-N.C.) has described the problem this way:

'Interrelationship' is the key word here. Once the correlating process begins on individual personal data in the many files of government, all the weaknesses and limitations of the computer as a machine will be operating on a grand scale to make possible a massive invasion of the privacy of millions, and it raises the spectre of a possible program of routine denial of due process. Interagency, inter-business networks are being established of computers that talk only to each other. Decisions affecting a person's job, retirement benefits, security clearance, credit rating or many other rights may be made without benefit of a hearing or confrontation of the evidence.

³⁴ Knisely, Robert A., "The Fruit of the Tree of Knowledge—Privacy Problems in Integrated Municipal Information Systems," Dec. 7, 1971, p. 7.

³⁵ Iowa's TRACIS (Traffic Records and Criminal Justice Information System), for example, will connect with the state's Department of Public Instruction, the Department of Social Services and others. And the California CLETS system... will be able to relate to records from the public schools.

³⁶ In recognition of this growing tendency and the immense data files available through his department, particularly those tied into social security numbers (as is the NCIC system), HEW Secretary Elliot L. Richardson has appointed an Advisory Committee on Automated Personal Data Systems to develop safeguards to "protect against potentially harmful consequences to privacy and due process." (See "Charter of the Secretary's Advisory Committee on Automated Personal Data Systems," Feb. 27, 1972.)

The computer reduces his opportunity to talk back to the bureaucrats. It removes his chances to produce documents, photographs or other evidence to alter a decision.³⁷

The problem of potential linkages between criminal justice systems and other governmental files on individuals has been centered in a debate that has plagued the new system since its inception. The NCIC guidelines initially required participating states to utilize computers "dedicated" to law enforcement uses only and managed by law enforcement personnel. Many of the states have opposed this policy on the grounds that dedicated computers cost more and, in some cases, that state law requires that all computer systems be centralized under the control of the governor.³⁸ According to Donald Roderick, Jerome Daunt's successor, the FBI will now permit each state to set its own rules in accordance with existing provisions for statewide computer administration. If a decision is reached to use a non-dedicated computer, however, that state must make a showing that the criminal justice data are under the control of law enforcement officials.

The Need for New Legislation

Neither the FBI nor LEAA, the two agencies of the Justice Department with the resources or powers to impose regulatory controls, has developed adequate safeguards for the fastgrowing computer files on criminal offenders. The NCIC guidelines are inadequate. As we have indicated, most of them are nonspecific, relying on state statutes to spell out specific protections. Since most of the states have no regulatory legislation on the books and the few laws that have been passed are inadequate, the system affords

³⁷ "The Computer and Individual Privacy," address of Sen. Sam J. Ervin (D-N.C.) to the American Management Association, March 6, 1967.

³⁸ Jerris Leonard sided with the states saying, "As long as I am here, we are going to carry out the philosophy of this administration and that is the states will decide what they need... If the FBI doesn't want to provide the service, we'll find someone else." (Washington *Evening Star*, Jan. 22, 1972). In addition the National Association for State Information Systems formally protested the dedication requirement to Attorney General Mitchell.

little protection against abuse. Further, the enforcement of the few NCIC standards that are binding depends exclusively on the FBI's willingness to exclude a noncomplying state from the system. This ultimate sanction has never been invoked.

Project SEARCH developed more comprehensive privacy and operational guidelines,³⁹ but these guidelines are advisory only, and not legally binding on the states. LEAA has been unwilling to impose the SEARCH standards as a condition of its grants. It has simply suggested that states contemplating the purchase of information systems with LEAA money "ensure that adequate provisions are made for system security, for protection of individual privacy and the insurance of the integrity and accuracy of the data collection."

Congress anticipated the need for regulation of the growing law enforcement information network in 1970 and added an amendment to the Safe Streets Act requiring LEAA to submit legislation by May 1, 1971, to ensure:

The integrity and accuracy of criminal justice data collection, processing and dissemination systems funded in whole or in part by the federal government, and protecting the constitutional rights of all persons covered or affected by such systems.

On Sept. 20, 1971, Senator Roman Hruska (R-Neb.) introduced S 2546, "The Criminal Justice Information Systems Security and Privacy Act of 1971," on behalf of the Administration. The bill essentially would codify the standards established by the NCIC policy board and give the Attorney General the authority to alter the scope of the national system as he deems necessary. The bill, which has been severely criticized for failing to provide adequate protection against misuse of data, was never assigned to an appropriate subcommittee for hearings.

In addition in 1970 Congress mandated the creation of a National Commission on Individual Rights to study, among other things, the impact "of the accumulation by law or required by

³⁹ See Technical Report No. 2, July 1970, "Security and Privacy Considerations in Criminal History Information Systems," prepared by the Project SEARCH Committee Security and Privacy. The committee has also prepared a model state statute and model regulations for the governance of state information systems. These have been introduced but not acted upon in several state legislations.

executive action" and to determine which practices "are effective, and whether they infringe upon the individual rights of the people of the United States." (Title XII, The Organized Crime Control Act of 1970.) This provision has never been implemented.

There are serious questions whether the state and national computerized files are necessary, whether they are worth their cost, both social and financial, and whether they work. Perhaps with more experience the FBI or LEAA will develop a convincing case concerning the manner in which the computerized information systems have developed. However, the Justice Department has not yet confronted the very real problems that the new NCIC system is creating, particularly in regard to governmental overreaching, invasions of privacy and infringement of basic constitutional rights.

Underlying the deficiencies of the new NCIC criminal offender records system is the vagueness of the legislation under which it operates. 28 USC §534 enables the Attorney General to set up (and alter) a system to "acquire, collect, classify and preserve identification, criminal identification, crime and *other records*," and to "exchange these records with, and for the official use of, authorized officials of the federal government, the states, cities and penal and *other institutions*." (Emphasis added.) The statute contains no standards; and despite the fact that the Attorney General has full power to do so, no regulations have ever been issued to govern the information system except to delegate the Attorney General's administrative authority to the FBI (28 CFR § 0.85).

In addition to the question of the Justice Department's statutory power, several aspects of the system as it is presently administered raise important constitutional questions. To include information unrelated to criminal convictions in the state files (and by automatic referral in the national file) may well violate the First Amendment and the due process and equal protection clauses of the United States Constitution.

For example, on numerous occasions the Supreme Court has held or indicated that the Fifth and Fourteenth Amendments' guarantee of due process protects individuals from injury caused by public bodies acting without giving the individual the opportunity to challenge or clarify the factual assumptions on which the agency is

operating.⁴⁰ The protection against arbitrary action and the right to be heard apply even when the activities involved do not entail direct civil or criminal penalties, and extend to the circulation by the government of prejudicial information.

In *Joint Anti-Fascist Refugee Committee v. McGrath*,⁴¹ the Supreme Court confronted a situation remarkably similar to that posed by certain aspects of the present-day Justice Department data distribution program. Ruling that the Attorney General must provide an opportunity for a hearing before including an organization on his subversive list, Justice Felix Frankfurter stated:

The heart of the matter is that democracy implies respect for the elementary rights of men, however suspect or unworthy; a democratic government must therefore practice fairness; and fairness can rarely be obtained by secret one-sided determination of facts decisive of rights. . . . No better instrument has been devised for arriving at truth than to give a person in jeopardy of serious loss notice of the case against him and opportunity to meet it. . . . The Attorney General is certainly not immune from the historic requirements of fairness merely because he acts, however conscientiously, in the name of security. 341 U.S. at 110-114.

Under the new NCIC system the federal and state agencies which disseminate background intelligence information or data pertaining to arrests not followed by conviction, without giving the subject the chance to clarify or correct his record, could be found in violation of the due process clauses of the Fifth and Fourteenth Amendments.

⁴⁰ See, e.g., *Joint Anti-Fascist Refugee Committee v. McGrath*, 341 U.S. 123 (1951); *Greene v. McElroy*, 360 U.S. 474 (1959).

⁴¹ *Supra*, n. 40. Although the Attorney General was ordered to institute proper procedures before adding an organization to the subversive list, the majority of the Court did not join any one opinion. Justice Frankfurter's constitutional reasoning has become the most noted of the opinions entered in that case. In *Wisconsin v. Constantineau*, 400 U.S. 433 (1971), the Supreme Court held unconstitutional a Wisconsin statute authorizing local authorities to post public notices prohibiting the sale of liquor to persons who drink excessively, without affording the interdicted individual a right to challenge the determination.

It is also quite possible that the NCIC criminal history file violates the equal protection clause, by magnifying the consequences of present discriminatory police practices. Because the data it collects focus on street crimes and offenses that tend to be committed by the disadvantaged and minorities, and because of its indiscriminate inclusion of data on arrests for ill-defined crimes (such as arrests for suspicion) and arrests not followed by charges or convictions, the NCIC file reinforces the existing class and racial bias of the criminal justice system. Arrests for "suspicion" or "investigation," for vagrancy and other vague crimes, constitute a major form of police discrimination against blacks and Chicanos. Keeping permanent computerized files of such arrests (and in some cases convictions) adds another layer of discrimination to the criminal justice system, encouraging surveillance, the imposition of stiffer penalties, etc., on minorities. When such records are made available to employers, discrimination in the hiring process is compounded. (See *Gregory v. Litton Systems*.)⁴²

CONCLUSIONS AND RECOMMENDATIONS

LEAA is investing substantially in the creation of a national computerized criminal offender information file serving state and local contributors and users. The files at present contain too much information and are accessible to too many agencies, including private business concerns. Few safeguards protect legitimate rights of personal privacy or prevent use of the information in a discriminatory manner. Standing alone, the new information systems require immediate and comprehensive regulations and controls. The potential harm that they could inflict, however, is

⁴² 316 F. Supp. 401 (C.D. Calif. 1970). The President's Commission on Federal Statistics, Vol. II (1971), p. 546, reported: "An applicant who lists a previous arrest faces at best a 'second trial' in which, without procedural safeguards, he must prove his innocence—at worst the listing of the arrest disqualifies him *per se*. The arrest record is the first of a series of 'status degradation ceremonies' in the criminal law process." The Commission pointed to the fact that in a recent survey of 39 countries not one lists arrests that have not led to convictions. "The 'criminal record' in these 39 countries includes only convictions, and often only those for serious crimes." (p. 548) For a detailed treatment of the problems inherent in the broad dissemination of arrest records, see *Security and Privacy of Criminal Arrest Records*, Hearings before Subcommittee No. 4 of the House Committee on the Judiciary, 92nd Congress, 2nd Session (April 1972).

made even more critical by (a) the coincident development of new state-level intelligence files on civil disorders and dangerous persons that are maintained by the same agencies that administer the information files and that are accessible to participants in the national system, and (b) the rapid expansion of computerized records on individuals maintained by welfare, health, education and other public and private agencies that can be (and have been) readily interfaced with the criminal offender files. To ensure integrity and fairness of such systems:

No further federal funds should be distributed for the operation, expansion or development of state and/or national information systems prior to the completion of a study by a neutral and reputable scientific body—such as the National Academy of Sciences or the National Commission on Individual Rights—setting forth the policy options facing the nation in regard to such systems. In particular, the study should examine: the necessity for various possible kinds of information (and intelligence) systems to effective law enforcement; the most appropriate structure(s) for such systems (centralized, decentralized, state controlled, law enforcement controlled, etc.); the kinds of safeguards that can and should be built into such systems; the relationship of the data banks developed under such systems to other data banks; and the proper forms for public regulation of such systems.

If a national or multi-state criminal justice information system is found to be justified after the full report by the independent body, federal legislation should be passed creating an affirmative right to privacy, which would require the government to justify in advance any activity that would conflict with that right. In addition, regulatory laws should be passed to control all information systems (1) developed and maintained by agencies of the federal government, (2) operated by state or local agencies but supported wholly or partly by federal funds and (3) interfacing with federal systems or federally supported systems. (If such legislation is not passed, the Attorney General should issue formal regulations under his present powers.) Among the kinds of safeguards that should be considered for inclusion in the legislation are the following:

- The legislation should spell out with specificity (rather than defining by exclusion) the scope of the criminal

history offender files and the matter to be included therein. Only serious crimes that pose actual danger to the public and are likely to involve interstate mobility should be included.⁴³ The national file should contain only identifying data, records of active arrests, convictions and sentencing and an identification of the state agency maintaining the full records. Records of arrests not followed by indictment or information within one year, or conviction within two years, should be deleted from the files. When a criminal law is repealed, the record of prior violations of it should be deleted from the computer. An affirmative obligation should be placed on all participating states to delete such information from their own files as well as the FBI files. Failure to do so should result in termination of participation in the system and imposition of financial penalties.

- Specific congressional approval should be required for any expansion or modification of the initial system, such as a decision to interface with other data banks within the Justice Department or other federal agencies.
- The legislation should provide for operation and/or monitoring of the national system by an independent agency or commission that would conduct audits and spot-checks on both the operating agency and the contributing agencies, and would report annually (and periodically, as requested) to Congress. The commission, which should include constitutional lawyers, representatives of citizens' groups and other civilians, would share responsibility with the operating agencies for the development of detailed guidelines to govern the operation of the system. No state should be allowed to participate in the federal system until such time as it has passed its own statute reflecting the national standards, creating a state monitoring body and providing for the protection of individuals whose records are included in the system.

⁴³ This would remove most victimless crimes from the file as well as the other petty offenses that are most subject to enforcement patterns that are socially discriminatory.

- *Each individual should be granted the right of access, notice and challenge to all information pertaining to him. A person should receive notification when his file is opened, and upon each entry he should be informed of his right to access and challenge. During a challenge, to protect the individual from incomplete and inaccurate information, an embargo should be placed on use of the information.*
- *The legislation itself should establish general standards for the operation of the system and should require the Attorney General to issue more specific, mandatory regulations to govern dissemination of the information to criminal justice agencies, the courts and corrections institutions and other public agencies. The information should be graded so that only the summary computer record (not access to supplementary state investigative files) will be available to certain recipients, such as federal and state employers, or courts seeking to determine sentences.⁴⁴*

⁴⁴The legislation should probably also waive sovereign immunity on behalf of the United States and make them jointly liable with any individual who disseminates information to an unauthorized recipient, on a strict liability basis. The law should include minimum damage penalties, attorneys' fees, and a provision for treble damages; the individual defendant and the governmental employer shall have the burden of proving a good-faith effort to make sure that the recipient did have authority to request and receive the information, in order to escape punitive and treble damages. The same sanctions should apply for dissemination of erroneous information. U.S. district courts should be given jurisdiction without regard to the amount in controversy.

APPENDIX F

Correctionetics: A Blueprint for 1984

DANIEL H. LUFKIN*

The American Justice Institute of Sacramento, California, working under a grant from the National Institute of Mental Health, completed in 1972 a six-volume report¹ of a three-year study of "the utilization of advanced information system technology as a means of improving the correctional decision-making process." The aim of the study was to design a system to enable managers of correctional institutions to make completely objective decisions about the treatment and disposition of criminal offenders. The study was the work of the Institute's Correctional Decisions Information Project (CDIP), whose epigraph is inscribed on the second cover of Volume I of the report:

*"TODAY AN INFORMATION SYSTEM HOLDS FOR
CORRECTIONS THE SAME BREAKTHROUGH POTENTIAL
AS DID THE MICROSCOPE FOR BIOLOGICAL SCIENCES
YESTERYEAR."*

It must in no way demean the dedicated and intelligent effort of the CDIP staff to point out that any project that aims to create an automated personal data system to monitor and control the popula-

*Staff Consultant to the Committee

¹Correctional Decisions Information Project, *Correctionetics: Modular Approach to an Advanced Correctional Information System* (Sacramento, Calif.: American Justice Institute), 1972.

tion of a prison efficiently necessarily creates a system with all the earmarks of the worst surveillance data bank any civil libertarian could imagine. CDIP has completed much of the work needed to reduce 1984 to practice. Simple substitutions of the words "governmental" for *correctional*¹ and "citizen" for *offender*² in the following excerpts from the CDIP report transforms serious and humane objectives for prisoners into a nightmare for citizens.

[C]orrectional administrators... must be able to... determine the ability of each operational program to assist various types of *offenders* toward *correctional* goal attainment. Such an ability is totally dependent upon information. Thus, information is power to withstand irrational, unjustified onslaughts. Information is power to confirm constructive policy decisions. Information is power to provide leadership for a rational approach to an improved *correctional* process. (Vol. 1, pp. 1-2).

The *Correctional* Information System portrayed in these documents is for that breed of managers which strives for an increasingly effective efficient, and responsive approach to rational, humane control and reintegration of *offenders*. Vol. 1, p. 6)

The recycling approach, or Correctionetic concept of successive approximations to desired goal attainment, is not limited to the management of *corrections*. It applies equally well to individual *offenders* as they strive to achieve their objectives on any of a number of dimensions of personal adjustments, e.g., vocational, marital, leisure time/social, or academic. (Vol. 1, p. 7)

This type of decision-making assistance is possible for *correctional* managers as they perform the following basic functions which constitute the management process:

1. Goal Definition
2. Planning

¹ Not italicized in original text.

² Not italicized in original text.

3. Operations Control
4. Achievement Assessment
5. Effectiveness Evaluation (Vol. 1, p. 8)

The last paragraph betrays the weakness of the transformation: if we assume that the CDIP system could apply as well to a nation as to a prison, we are also assuming that "management" and "government" are interchangeable. In fact, however, the idea of the social contract, of authority derived from the consent of the governed (rather than from the managed), is precisely what differentiates a nation from a prison.

Valuable as a more thorough exploration of that differentiation might be, we shall forego it here in order to concentrate on the practicalities of the CDIP approach in the context of a special micro-society into which the problems of citizens' rights and privacy do not immediately intrude. Nevertheless, the conditions of prisoners and of free citizens are not diametrically opposed: prison and 20th-century America are not the end points on any scale of social values. Prisoners do have rights and privacy just as ordinary citizens have restrictions and intrusions. Correctionetics includes data on an offender's religion and sexual practices, but none on the contents of his letters or his conversations with his lawyer. Correctionetics is thoroughly benevolent, and efficient benevolence is precisely the characteristic that seems to lie at the root of our suspicions of the computerized state.

At the heart of Correctionetics is the capability for what CDIP calls *demand reporting*: the capability of producing from a generalized data base a report whose content and structure fit the needs of one particular decision. In such a system, the capability of generating routine reports with fixed content is implicit. In the correctional context, for example, the manager may request a report listing the total number and names of offenders in a particular institution who have been convicted of a certain crime, who have served their minimum sentence, are in a given range of age, and who have a particular occupation or skill. Such a report would simplify matching offenders eligible for release with known job possibilities outside. In the civil context, a demand request might be for a list of the blond males in their late thirties who drive blue Pontiacs with the last license digit of seven. The motive of the

request is not the offer of a job, but rather the search for a bank robber.

The capability of a data system to perform such a search clearly rests on two features: a comprehensive file of personal characteristics, and the logical ability to compare the file contents with the terms of the request. Both these capabilities are easy to build into a computer system; in theory there is no difficulty at all in setting up a system of considerable range and depth. Experience tells us, though, that real life consistently falls short of expectations. It is instructive to see how this universal principle operates on Correctionetics and to extrapolate that knowledge to the real world.

Offender Data File

The underlying operating unit of Correctionetics is the *offender data file* (ODF), a record of 369 different facts and opinions about the offender. When the CDIP study first began, in July 1969, the ODF included only 200 data elements. Let us note for later reference that the number of data elements found to be needed nearly doubled in about two years of planning and experimental operation of the system. The ODF begins with the name (and aliases) of the offender, three identification numbers, his date and place of birth, his first year of State residence, his ethnic origin, and his religious preference. This much information, the *offender identification block*, requires 139 characters of file space as a minimum for each offender. (The average offender was found to have 2.6 aliases at 33 characters per alias, and some had as many as 12.)

The ODF goes on to record the legal status, the offense history, the medical, dental, psychological, psychiatric, academic, vocational, and adjustment histories of the offender, details of his childhood, his family and its economic status, his work history in the institution, and his prospects for release and parole. The data are grouped into 17 blocks and occupy a minimum file space of 1134 characters, but the complete ODF would easily fit on a single page of typescript, since most of the information is entered in coded form.

Coding data in order to conserve storage space and to make possible a logical search for a known data entity is characteristic of computer data processing. The extent to which the coding con-

ventions match the underlying structure of the data determines to a very great extent the ultimate power of the computer program to handle any but the simplest sorting tasks. The coding manual for building the ODF provides explicit codes for every coded data element. Since the computer's perception of the real world takes place only through the medium of the codes (outside of literal data such as names and the like), the structure of the codes and selection of the code elements must be made with the greatest care and foresight.

In the experience of practically every organization that has developed a sizable computer data base, one of the greatest expenses in the operation comes in converting the data from conventional manual to encoded machine-accessible form. Conscientious, accurate coding demands well-trained, highly motivated clerks who can keep an extensive body of coding rules in mind and apply them quickly to an amorphous mass of real-world facts.

In the CDIP work, the coding manual is a 200-page volume explaining every possible entry in the ODF. The scope and structure of the codes themselves have apparently never been tested by processing a large number of actual correctional records, although we shall later discuss a greatly restricted pilot program and its results. The coding manual shows the extent to which standardized codes for occupations, school subjects, diseases, and similar common data entities have already been adopted among independent but parallel data-processing organizations. Academic course codes are those of the California Department of Education, and include not only introduction to data processing (MXA) and computer techniques (MXB), but also a very full range of elementary and secondary school subjects. The vocational training codes are those used in Federal government job classifications. The Federal code is considerably edited to provide a fuller breakdown of skills important to prison operation: laundry workers (36x.xxx), farm workers (2xx.xxx), food workers (52x.xxx), mattress inspectors (780.687), and the like. (There is no code provision for locksmith.) Medical diagnosis and treatment is coded according to the American Medical Association's *Standard Nomenclature of Diseases and Operations*. The codes for voluntary and leisure time activities presumably reflect the choices available to actual inmates of the California correctional system. They include all the familiar sports plus some

surprises, such as bicycle racing (103) and golf (111). Special-interest groups include aviation (706) and transactional analysis (726). That an activity code for the classification of prisoners can hold surprises is a good indication that a similar code for the public at large would run to many times 200 pages.

Data for Decision Making

During the course of the CDIP study, two pilot programs were carried out to test the preliminary design of the system and to demonstrate the operation of the system before experienced correctional managers. The results of those programs are interesting as an indicator of the potentials and pitfalls we could expect to meet in a large-scale general system.

In testing some of the preliminary design concepts of the system, CDIP planners identified the following factors in decision-making processes that use data in the way they can be provided by a large-scale computerized system:

- Decision makers say they need data concerning large numbers of variables.
- Empirical studies indicate that the decision-making process actually involves a small number of variables, six or eight at the most.
- The structure of the decision-making process itself and the order of presentation of the data both affect the outcome.

These and other more peripheral problems were tested in an experimental setting with data records of actual prisoners presented to experienced correctional officers in a simulation of computer operation. The officers decided on the disposition of three hypothetical cases: granting a minimum-security custody rating; granting a parole after a minimum sentence had been served; and revoking a parole after a borderline violation. The type of data, its order of selection, and its weight in the ultimate decision were all recorded.

The detailed analysis of the experiment appears in Appendix D of the CDIP report; it is enough here to summarize the findings which would have broader applicability to a similar task in a citizen data bank.

- The decision makers did in fact use an average of only eight pieces of data. There were a number of data items which were never looked at, even though they had been specifically requested in the data bank.
- For the decision on custody rating and granting parole, the record of the offense itself was the first thing considered. For revoking parole, the offense was second. In general, purely factual data on the offender's history were used more than subjective data derived from evaluation of the offender by the correctional staff.
- Deeper statistical analysis of the decision-making process revealed no underlying regularities in the way decisions were made, which regularities many data-processing specialists assume to exist.

Data for Reports

In the second pilot test, the capabilities of a computer program package much more restricted than the full, planned correctionetics system were demonstrated to meetings of senior correctional officers at their national conventions. A special 74-item ODF was prepared from the conventional records of 5756 offenders in a cross section of the institutions of the California Department of Corrections. It is worth noting that the project found it necessary to "embellish" (CDIP's word) the original data to make them conform to the requirements of the demonstration.

In the first demonstration, at Palm Springs, a computer at Santa Monica was loaded with the data base and the demonstration programs. The terminal at Palm Springs was connected to the computer by telephone. The demonstration programs were relatively simple sorting routines which demonstrated how to generate a list of offenders to be released in the next month, and then searching the ODF for a qualified inmate to take over a clerk's job vacated by a releasee. After the prepared program application was demonstrated, the spectators were allowed to make up their own queries for the data, although it is not clear from the report what these queries were or how well that part of the demonstration worked.

The second demonstration of the same program package was held in Cincinnati. It is a keen comment on the computer specialist's faith in his charges that the CDIP staff took the precaution of

punching all the query input on paper tape beforehand, so that a keyboard mistake—alas! all too common—would not upset the demonstration. The staff also took the precaution of punching the computer's *output* on paper tape beforehand and taking that tape with them to Cincinnati. There, the output could be fed into the teletype printer under the control of a foot-switch, thus simulating the action of a computer at the other end of the line without exposing the demonstration to the dangers of real-life computer operation. (It is also a tribute to the candor of the CDIP staff that they fully describe this ploy in their report.) The demonstration ended with a period of genuine computer operation over the link, during which the audience had an opportunity to try the system. Typical queries from the experienced correctional officers dealt with average time served by offenders in various classifications of confinement, profiles of offenders involved in escape attempts, juvenile commitment history of selected sets of adult offenders, and other similar sorting and listing tasks.

Correctionnetics as a Data Bank

What does this report about Correctionnetics, an automated personal data system designed for a prison society with few of the traditional concerns for privacy, have to tell us about computers and privacy in our own wider society? Are we looking at a worst-case microcosm, one from which we can no more extrapolate to our present civil society than we can from an anthill? Even as an anthill can teach us something about living beings in general, so can Correctionnetics teach us something about the intrinsic limitations computerized personal data systems have, even in the absence of manifest safeguards for privacy.

Let us look at some of the features of Correctionnetics and compare them with roughly corresponding features of other personal data systems.

Scope. First, and of fundamental importance, Correctionnetics stores no more data on an individual prisoner than the manual system did. In point of fact, it stores less. When the records of the sample population were being prepared for the demonstrations, it was necessary to omit all but a tiny fraction of the material in the prisoners' record jackets, many of which were half a foot thick. The material omitted was that least suited to computer treatment; that

is, anecdotal and narrative records, interview reports by psychologists, extracts from correspondence, and the like. It is this sort of intelligence record that is fundamentally unsuited for computer treatment, and which would have the greatest potential for harm to privacy if it were to enter the lightly protected files of a computer data bank.

Costs. Second, Correctionnetics seems to be so grossly uneconomical that there would be little incentive to adopt it in a full-scale way. As every business comptroller knows, it is almost impossible to price out a computer system before it goes into operation, and difficult enough even to measure the running operating costs. The CDIP report is reticent on costs, but we would estimate the storage and processor requirement for an offender population of 50,000 to be over 250,000,000 bytes (CDIP Table 5.4.2). Roughly corresponding commercial credit experience suggests a cost of about \$80,000 per month to which staff and overhead costs would add about 50 percent to bring the total cost to about \$120,000 per month. It is hard to see that the advantages of automated prison management on the scale suggested by CDIP would be defensible unless it could be carried as a partial load on some larger general-purpose system.

Impact on Decision Making. Third, the impact of Correctionnetics on the actual process of prison management decision making does not seem to be all that striking. It is obvious that the computer has no difficulty in finding, for example, the average age of narcotics offenders in a particular institution, but one suspects that the warden could guess the figure closely enough for practical purposes with no aid at all. For particular tasks, such as matching parolees with job openings, the services of a computer are well defensible, but more economically carried out in a special-purpose system that only handles employment data and need not process the excess baggage of the rest of the offender data file merely to arrive at a job match. This illustrates a point that deserves emphasis again and again in designing data-processing systems: a system should be no larger than needed to do a particular task. Money spent to provide capacity for the possibility of data processing in the abstract, or merely to provide "management information" is like wagering at unknown odds. A management information program run once or

twice a month on a computer system that otherwise earns its keep on accounting, payroll, and inventory yields impressive decorations for the board room and likely does no harm. But neither does it do enough good to deserve a dedicated computer system all to itself.

Safeguards for Correctionetics

Finally, we may look at Correctionetics as a test case for the application of safeguards. What effects would there be if Correctionetics gave offenders more control over information about themselves?

In the Correctionetics system there is no provision for feedback from the data subjects. The prison management's goals are defined in terms of data measurements made through the system, and the system is then used as the means of bringing operations of the prison into conformity with those goals. If a data error creeps in from any source, the system can produce a false measurement or a false operation or both; without suitable feedback, the false measurement may well reinforce the false operation instead of correcting it.

Let us look at an example as it might actually run through the Correctionetics system. Through a coding error, a prisoner's file is changed to show that he is an active homosexual. A status change report is automatically generated which removes him from a television repair course (forbidden to sexual offenders) and transfers him to a cell in a more secure block (because a profile of such offenders shows them to be, on the average, more aggressive than others). These two actions confirm the prisoner's suspicions about the prison administration and he fulfills their expectations by actually becoming sullen and aggressive, which behavior, in turn, generates another automatic transfer order to an "adjustment center." In this scenario, and in a hundred others we could imagine, an originally minor error in a record has snowballed into serious injustice.

Giving the prisoner a right to know what information his file contains would have had the immediate effect of discovering the error, provided he realized that some change in that information had taken place. In this case, the change in training status would have been an obvious clue to him. A right to secure correction of the data would have stopped its propagating in the program and

would have prevented or undone the subsequent actions the system made on the basis of the error.

Thus, the possibility of feedback from the data subject to the data bank can act as a powerful brake on the freedom of an authority to take arbitrary action. It is obvious that this would have clear benefit for a person at the bottom of the heap, but we wish to point out that it also protects the authority taking action. If we make the assumption that administrative injustice will eventually come to light and be dealt with through the law, it is very much to the benefit of the warden, in our example, to insure that his decisions are based on the best data he can command. Rules to ensure that errors in personal data banks are discovered and corrected promptly will go far toward preventing abuse of even so stern a system as Correctionetics.

Computerized Decision Making

The deeper question of the actions that an automated system such as Correctionetics can take on the basis of even perfect data also deserves careful consideration. In our example from the actual program, a record as a sexual offender was automatically treated as sufficient cause to disqualify an inmate from training as a television repairman. This is a simple decision to program, and one presumably based on an actual rule of the California Department of Corrections. In pre-automation practice, the application of such a rule would usually take place in a context such that knowledge of other factors in the offender's record would come to the attention of the training officer. He might give the rule only as much weight as he thought appropriate in the light of all the factors in an individual case, and could certainly at least take initiative to seek occasional exceptions from the rule.

It is precisely that sort of personal initiative which seems to be the most strongly appreciated advantage of human over computerized administration. Although we have all experienced occasions in which a bureaucrat acted like a computer, we also recognize those occasions as the exceptions to our usual experience with human decision making.

To be fair, it is possible in theory to program a computer to simulate human decision making. In practice, though, it is obvious from the Correctionetics experiment that we are far from attaining that end.

Appendix G

The Law Relating to HEW Personal-Data Record Keeping

Introduction

The Federal law bearing on collection, storage, handling, dissemination, and other use of information about individuals (hereinafter often referred to as "personal information activities") is a large and varied assortment of statutes, regulations, Executive orders, and other directives. Little of this law applies generally to all agencies of the Federal government, and still less has general application to personal information activities of organizations outside the Federal government.

This paper discusses the law that governs the behavior of the Department of Health, Education, and Welfare¹ (hereinafter referred to as "the Department" or "HEW") and its grantees and contractors in the conduct of personal information activities.

Three statutes of general application throughout the Federal government are discussed with special reference to their HEW effects: the Federal Reports Act, 44 U.S.C. 3501 *et seq.*; the so-called "Freedom of Information Act", 5 U.S.C. 552; and a

¹ The Department comprises a number of organizational components through which its operational programs and activities are carried out, *viz.*: the Public Health Service (PHS), consisting of the Food and Drug Administration (FDA), the Health Services and Mental Health Administration (HSMHA) and the National Institutes of Health (NIH); the Education Division, consisting of the National Institute of Education (NIE) and the Office

criminal statute forbidding government officers and employees from making unauthorized disclosures of information. 18 U.S.C. 1905. This paper focuses on personal information and does not cover the law relating to trade secrets or commercial information.

The *statutory* sources of authority relating to HEW's conduct of personal information activities may be categorized as follows: (1) broad authority to administer and manage HEW; (2) authority for HEW to carry out particular program activities, including research, whether conducted by HEW or by others with support from HEW; (3) authority for HEW information (or personal information) activities; (4) authority (sometimes by Executive order rather than by statute) which, though not directly conferring authority on HEW, gives rise indirectly to obligations imposed on HEW, commonly along with other government departments, to obtain, provide, and/or report personal information for its own purposes or to other government departments or agencies (e.g., Civil Service Commission, Internal Revenue Service) to the Congress, or to the public. Except in category (3), these sources of authority generally make no explicit reference to information (or personal information) activities, but it is a reasonable and necessary interpretation of the authority to include such activities.

Sources of authority for HEW's personal information activities are legion, resulting particularly from the necessity of interpreting such authority to exist in all statutes concerning program activities and research covered by category (2). This paper seeks to present a complete compilation of the sources of authority for HEW's personal information activities in categories (1), (3), and (4). With respect to category (2) it discusses only statutes that have special significance in relation to personal information activities or contain a provision relating specifically to personal information activity. It should be noted that in order to perform statutory program duties, it is often necessary to conduct personal information activities, particularly in programs that provide direct services to individuals, for example, the repatriation assistance programs of the Social and

of Education (OE); the Social and Rehabilitation Service (SRS); the Social Security Administration (SSA); and the Office of the Secretary (OS), consisting in part of the Office for Civil Rights (OCR), and the Office of Human Development, which includes the Administration on Aging (AoA), the Office of Child Development (OCD), and the Office of Youth Development (OYD). (Effective July 1, 1973, the operating agency constituents of the Public Health Service will be reorganized to consist of the Food Drug Administration, the Center for Disease Control, the Health Resources Administration, the Health Services Administration, and the National Institutes of Health.)

Rehabilitation Service, 24 U.S.C. 321-29, and section 1113 of the Social Security Act, 42 U.S.C. 1313. In addition, authorized research activities, for example in the health fields, frequently require extensive information about individuals. Examples of authority for the "conduct and support" of research activities include the statutes authorizing the research institutes of the National Institutes of Health. Public Health Service Act sections 402 (Cancer, 42 U.S.C. 282), 412 (Heart Diseases, 42 U.S.C. 287a), 422 (Dental Diseases, 42 U.S.C. 288a), 431 (Arthritis, Rheumatism, and Metabolic Diseases, Neurological Diseases and Stroke, and other particular diseases and groups of diseases, 42 U.S.C. 289a), 441 (Child Health and Human Development, 42 U.S.C. 289d), 442 (General Medical Sciences, 42 U.S.C. 289e), 451 (Eye Diseases and Visual Disorders, 42 U.S.C. 289i).

Because the statutes deal sparingly with personal information activities, one must also turn to regulations that have been issued to implement statutes to get a fuller understanding of the authority that governs such activities. We have sought to identify and discuss the principal regulations that have operational significance for the conduct of personal information activities, including all that are Departmental in scope (i.e., apply to all operating agencies of the Department) and those that apply throughout a particular operating agency. Of regulations limited in application to a particular program or activity, we have attempted to include only those that contain specific provisions about personal information activities. Guidance as to HEW personal information activities appears also in program materials issued at the operating level which are more detailed than statutes or regulations but which may lack the force of law. The discussion of such materials in this paper is limited to a few examples.

The law relating to personal information activities carried out in connection with HEW personnel administration is treated separately, because the legal requirements and operational considerations involved are distinctive.

Authority to Collect Information

GENERAL

The Department was created by Reorganization Plan No. 1 of 1953 which became effective on April 11, 1953 (67 Stat. 18) and is

recognized as an executive department in 5 U.S.C. 101. The Plan provides that the Department shall be administered under the supervision and direction of the Secretary. A general grant of power enables the Secretary to act as he finds necessary in order to carry out his responsibilities in the areas of health, welfare, social security, and education. An opinion of the Attorney General, discussing general Secretarial powers, emphasized that express statutory authority is not required for every administrative act. 28 Op. Atty. Gen. 549 (January 5, 1911). The Secretary's responsibilities are further defined in part in 5 U.S.C. 301 which states:

The head of an Executive department . . . may prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property.

See also section 215(b) of the Public Health Service Act, 42 U.S.C. 216(b), setting forth similar authority to promulgate regulations for administration of the Public Health Service, including regulations relating to custody, use and preservation of records.

In addition to the Secretary's general authority to manage the Department, there are numerous specific statutory provisions authorizing collection of information by HEW. The authority for the conduct of programs characteristically requires that HEW make periodic reports on the conduct and status of those programs. In addition, where HEW is authorized to contract with or grant money to States, localities, and private institutions for the conduct of programs, the legislation generally requires them to make periodic reports to the Department or its agencies. See, e.g., Elementary and Secondary Education Act, section 142(a) (3), 20 U.S.C. 241f(a) (3), (periodic reports to the Commissioner of Education evaluating effectiveness of Title I payments).

EDUCATION

Perhaps the broadest grant of authority for collection of information is the Organic Act of 1867, 14 Stat. 434, which established a "Department of Education"

. . . for the purpose of collecting such statistics and facts as shall show the condition and progress of education in the

several States and Territories, and of diffusing such information respecting the organization and management of schools and school systems, and methods of teaching, as shall aid the people of the United States in the establishment and maintenance of efficient school systems, and otherwise promote the cause of education throughout the country. See 20 U.S.C. 1.

Under more recent education laws the Commissioner of Education is charged specifically with collecting and disseminating information. Section 422(a) of the General Education Provisions Act provides:

The Commissioner shall—

(1) prepare and disseminate to State and local educational agencies and institutions information concerning applicable programs and cooperate with other Federal officials who administer programs affecting education in disseminating information concerning such programs;

(2) inform the public on federally supported education programs;

(3) collect data and information on applicable programs for the purpose of obtaining objective measurements of the effectiveness of such programs in achieving their purposes; and

(4) prepare and publish an annual report (to be referred to as "the Commissioner's annual report") on (A) the condition of education in the nation, (B) developments in the administration, utilization, and impact of applicable programs, (C) results of investigations and activities by the Office of Education, and (D) such facts and recommendations as will serve the purpose for which the Office of Education is established (as set forth in section 403 of this Act). 20 U.S.C. 1231a(a).

Other provisions relating to collection of information are found in section 417 of the General Education Provisions Act, 20 U.S.C. 1231f, and in section 501 of the Education Professions Development Act, 20 U.S.C. 1091. The former gives the Commissioner authority to furnish various information to, and to make special statistical compilations and surveys for, State or local officials,

private organizations, or individuals. The latter provides for the development of "information on the actual needs for educational personnel, both present and long range."

Although it seems clear that the foregoing provisions regarding information activities in the field of education do not contemplate the dissemination of identifiable personal information, such information may need to be collected in order to prepare the statistical compilation and analyses to be used or disseminated.

HEALTH

In defining the general powers and duties of the Secretary in the health area, section 301 of the Public Health Service Act states:

The Secretary shall conduct in the Service, and encourage, cooperate with, and render assistance to other appropriate public authorities, scientific institutions, and scientists in the conduct of, and promote the coordination of, research, investigations, experiments, demonstrations, and studies relating to the causes, diagnosis, treatment, control, and prevention of physical and mental diseases and impairments of man, including water purification, sewage treatment, and pollution of lakes and streams. In carrying out the foregoing the Secretary is authorized to—

(a) Collect and make available through publications and other appropriate means, information as to, and the practical application of, such research and other activities; 42 U.S.C. 241.

Further authority to collect information in the health field is provided in section 305 of the Public Health Service Act which authorizes the National Health Surveys and Studies as follows:

(a) The Secretary is authorized, (1) to make, by sampling or other appropriate means, surveys and special studies of the population of the United States to determine the extent of illness and disability and related information such as: (A) the number, age, sex, ability to work or engage in other activities, and occupation or activities of persons afflicted with chronic or other disease or injury or handicapping condition; (B) the type of disease or injury or handicapping condition of each

person so afflicted; (C) the length of time that each such person has been prevented from carrying on his occupation or activities; (D) the amounts and types of services received for or because of such conditions; (E) the economic and other impacts of such conditions; (F) health care resources; (G) environmental and social health hazards; and (H) family formation, growth, and dissolution; and (2) in connection therewith, to develop and test new or improved methods for obtaining current data on illness and disability and related information 42 U.S.C. 242c.

It should be noted that a provision was added to this paragraph by P.L. 91-515 to protect the privacy of persons supplying such information. (See discussion at p. 279, below.)

Section 317 of the Public Health Service Act, 42 U.S.C. 247b, authorizes support of communicable disease control programs, and calls for reports to the Secretary on communicable disease problems by grantees under the program.

Section 315 of the Public Health Service Act, 42 U.S.C. 247, authorizes the issuance of information related to public health.

Section 313 of the Public Health Service Act, 42 U.S.C. 245, directs the Secretary to “. . . . prepare and distribute suitable and necessary forms for the collection and compilation of [mortality, morbidity, and vital statistics] which shall be published as a part of the health reports published by the Secretary.” This section is authority for the operations of the National Center for Health Statistics of the Health Services and Mental Health Administration.

In addition there are programs involving health services which involve the collection of personal information (e.g., operation of Public Health Service hospitals, Public Health Service Act § 321, 42 U.S.C. 248; narcotics addict care and treatment, Public Health Service Act § 341, 42 U.S.C. 257).

The Secretary is authorized to “conduct examinations and investigations for the purposes of . . . [the Federal Food, Drug, and Cosmetic] Act” 21 U.S.C. 372.

Under the Federal Coal Mine Health and Safety Act of 1969, 30 U.S.C. 801-960, the Secretary has certain obligations with respect to the medical examination of coal miners. Under the Act, coal mine operators are obliged to provide miners with chest X-rays in accordance with instructions of the Secretary, and to provide the

Secretary with the results of the readings of such X-rays. Under the Act, the Secretary is obliged to provide the results of such readings to the miners involved. Sec. 203(a), 30 U.S.C. 843. There is no statutory obligation of confidentiality, but the Secretary's regulations for the program require mine operators to give assurance that they will not “solicit a physician's roentgenographic findings” and that they have instructed the physicians that duplicate X-rays will not be made. 42 C.F.R. 37.4.

WELFARE

The authority of the Social Security Administration (SSA) to collect information is derived primarily from its duty to carry out its program responsibilities. In this regard, Title II of the Social Security Act, Federal Old-Age, Survivors, and Disability Insurance Benefits (OASDI), provides in part as follows:

(a) The Secretary shall have full power and authority to make rules and regulations and to establish procedures, not inconsistent with the provisions of this title, which are necessary or appropriate to carry out such provisions, and shall adopt reasonable and proper rules and regulations to regulate and provide for the nature and extent of the proofs and evidence and the method of taking and furnishing the same in order to establish the right to benefits hereunder. Sec. 205(a); 42 U.S.C. 405(a).

* * * * *

On the basis of information obtained by or submitted to the Secretary, and after such verifications thereof as he deems necessary, the Secretary shall establish and maintain records of the amounts of wages paid to, and the amounts of self-employment income derived by, each individual and of the periods in which such wages were paid and such income was derived and, upon request, shall inform any individual or his survivor, or the legal representative of such individual or his estate, of the amounts of wages and self-employment income of such individual and the periods during which such wages were paid and such income was derived, as shown by such

records at the time of such request. Sec. 205 (c)(2)(A); 42 U.S.C. 405 (c)(2).

The Secretary is also authorized to obtain information for the purpose of any hearing, investigation or other proceeding authorized or directed under Title II of the Social Security Act or relative to any other matter within his jurisdiction thereunder, by use of the subpoena power if necessary. Sec. 205(d); 42 U.S.C. 405(d).

Section 218(e) (1)(B) of the Social Security Act, 42 U.S.C. 418(e) (1)(B), authorizes the Secretary to issue regulations prescribing reports by States under agreements extending OASDI coverage to State and local government employees.

Title XVIII of the Social Security Act, Health Insurance for the Aged (Medicare), authorizes the use of intermediaries and carriers for the administration of benefits and specifies that each contract shall provide that the intermediary or carrier shall furnish to the Secretary information it obtains in performing its functions and shall maintain records supporting such information § 1816(b)(2), 42 U.S.C. 1395h(b)(2), and § 1842(b)(3)(D) and (E), 42 U.S.C. 1395u(b)(3)(D) and (E). In addition, the Secretary is authorized to secure information "as may be necessary in the carrying out of his functions. . ." and directed to carry on studies relating to health care of the aged and to the operation and administration of the hospital and supplementary medical insurance programs for the aged. § § 1874 and 1875, 42 U.S.C. 1395kk and 1395ll.

The collection of information by SSA is closely related to some Internal Revenue Service activities and there is interchange of information between the agencies. See 20 C.F.R. 401.3 (d). Internal Revenue Act provisions and the regulations thereunder provide that:

Every person liable for any tax imposed by this title, or for the collection thereof, shall keep such records, render such statements, make such returns, and comply with such rules and regulations as the Secretary [of the Treasury] or his delegate may from time to time prescribe. Whenever in the judgment of the Secretary or his delegate it is necessary, he may require any person, by notice served upon such person or by regulations, to make such returns, render such statements, or keep such records, as the Secretary or his delegate deems

sufficient to show whether or not such person is liable for tax under this title. 26 U.S.C. 6001; Sec 26 C.F.R. 1.6001-1.

When required by regulations prescribed by the Secretary [of the Treasury] or his delegate any person made liable for any tax imposed by this title, or for the collection thereof, shall make a return or statement according to the forms and regulations prescribed by the Secretary or his delegate. Every person required to make a return or statement shall include therein the information required by such forms or regulations. 26 U.S.C. 6011(a); See 26 C.F.R. 1.6011-1.

The Administration on Aging has the "duty and function" to

(1) serve as a clearinghouse for information related to problems of the aged and aging;

* * * * *

(4) develop plans, conduct, and arrange for research in the field of aging

* * * * *

(6) prepare, publish, and disseminate educational materials dealing with the welfare of older persons;

(7) gather statistics in the field of aging which other Federal agencies are not collecting; Older Americans Act of 1965, § 202.

There is also the requirement, similar to that under Titles I, IV, X, XIV, XVI, and XIX of the Social Security Act (see p. 268, below), that a State agency administering a State plan program under the Older Americans Act will make reports to the Commissioner on Aging, ". . . in such form and containing such information, as the Commissioner may from time to time require." Older Americans Act of 1965, § 305(a)(3).

Information and reports authority also exists in the area of juvenile delinquency prevention and control. The Secretary is directed to "collect, evaluate, publish, and disseminate information and materials relating to research and programs and projects . . ." in the juvenile delinquency field. Juvenile Delinquency Prevention

Act, § 303, 42 U.S.C. 3873. Provision is made for continuing evaluation of programs and activities under the Act, which evaluations "shall include comparisons with proper control groups composed of persons who have not participated in programs" under the Act. Title IV, § 405, 42 U.S.C. 3885. The Act also requires an annual report to Congress on Juvenile delinquency activities including, among other things,

the number and types of training projects, number of persons trained and in training, and job placement and other follow-up information on trainees and former trainees Title IV, § 409, 42 U.S.C. 3889.

Each title of the Social Security Act authorizing a public assistance program contains a clause that the State plan for the program must

provide that the State agency will make such reports, in such form and containing such information, as the Secretary may from time to time require, and comply with such provisions as the Secretary may from time to time find necessary to assure the correctness and verification of such reports; Title I, Old Age Assistance and Medical Assistance for the Aged, § 2(a)(6), 42 U.S.C. 302(a)(6); Title IV, Aid to Families with Dependent Children, § 402(a)(6), 42 U.S.C. 602(a)(6); Title X, Aid to the Blind, § 1002(a)(6), 42 U.S.C. 1202(a)(b); Title XIV, Aid to the Permanently and Totally Disabled, § 1402(a)(6), 42 U.S.C. 1202(a)(6); Title XVI, Aid to the Aged, Blind, or Disabled, and Medical Assistance for the Aged, § 1602(a)(6), 42 U.S.C. 1382(a)(6); Title XIX, Medical Assistance (Medicaid), § 1902(a)(6), 42 U.S.C. 1396(a)(6).

There is a specific reporting requirement in section 402(a)(21) of the Social Security Act, 42 U.S.C. 602(a)(21), that the States send to the Secretary the names and social security numbers of parents who have a court-ordered obligation to support AFDC recipients, but who cannot be found. Under § 410 of the Act, 42 U.S.C. 610, the Secretary is to consult the Secretary of the Treasury to see if such parents can be located through Internal Revenue Service files.

Another authorization to collect information is found in the legislation establishing the Children's Bureau (a unit now placed in the Office of Child Development), which is charged with "investigating and report[ing] to the Secretary . . . upon all matters

pertaining to the welfare of children" Act of April 9, 1912, ch. 73 sec.2, 37 Stat. 79, 42 U.S.C. 192.

OFFICE FOR CIVIL RIGHTS

Executive Order 11246 (3 C.F.R. 342 (1964-65 Comp.), Sept. 24, 1965), which prohibited discrimination in employment practices by Federal contractors and subcontractors, provides that in every Government contract, in addition to the nondiscrimination clauses, the following clause shall be included:

(5) The contractor will furnish all information and reports required by Executive Order No. 11246 of September 24, 1965, and by the rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the contracting agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders. § 202.

In HEW, compliance with the Executive order is handled by the Office for Civil Rights (OCR). The Executive order provides that

Each contracting agency shall be primarily responsible for obtaining compliance with the rules, regulations, and orders of the Secretary of Labor with respect to contracts entered into by such agency or its contractors. § 205.

In addition, a section of the regulations issued by the Secretary of Labor pursuant to the Executive order provides that

The head of each agency shall, subject to the prior approval of the Director [of the Office of Federal Contract Compliance], establish a program and promulgate procedures to carry out the agency's responsibilities for obtaining compliance with the order and regulations and orders issued pursuant thereto. 41 C.F.R. 60-1.6(b).

The Director of the Office of Federal Contract Compliance is further authorized to redelegate authority given to him. Such re delegated authority "shall be exercised under [the Director's] general direction and control." 41 C.F.R. 60-1.46. One further

provision upon which OCR jurisdiction is based contains the definition of "compliance agency":

...the agency designated by the Director on a geographical, industry or other basis to conduct compliance reviews and to undertake such other responsibilities in connection with the administration of the order as the Director may determine to be appropriate. 41 C.F.R. 60-1.3(d).

This section continues with guidelines for when no such designation is made.

The Department of Labor regulations define the responsibilities of OCR for conducting compliance reviews, 41 C.F.R. 60-1.20, and complaint investigations. 41 C.F.R. 60-1.24 (b). The regulations also require such disclosure to OCR as is necessary to determine whether a contractor is complying with the Executive order. 41 C.F.R. 60-1.7 and 1.43.

OCR activities also include monitoring compliance with Title VI of the Civil Rights Act of 1964 which prohibits discrimination in programs and activities receiving Federal financial assistance. Under Title VI, Department regulations provide for the submission of compliance information to the Department by recipients of financial assistance and for access by Department officials to such information as is necessary to ascertain compliance with the Act. 45 C.F.R. 80.6. The regulations also require periodic compliance reviews and investigations of specific complaints. 45 C.F.R. 80.7.

Constraints on the Process of Collecting Information

Superimposed upon the authority of HEW to collect information is the Federal Reports Act, 44 U.S.C. 3501-3511, passed originally in 1942 (56 Stat. 1078). Section 3509 states that "A Federal agency may not conduct or sponsor the collection of information upon identical items, from ten or more persons, other than Federal employees, unless, in advance of adoption or revision of any plans or forms to be used in the collection—" the Office of Management and Budget (OMB) approves the proposed collection of information.

The stated purpose of this Act is to minimize both the burden upon those required to furnish information and the cost to the Government of collection. In addition, the Act provides for cooperation among agencies in sharing information. Provisions are included relating to unlawful disclosure and confidentiality of information. See p.p. 272-273, below. See generally OMB Circular No. A-40 Revised, May 3, 1973.

The Act defines "information" as

facts obtained or solicited by the use of written report forms, application forms, schedules, questionnaires, or other similar methods calling either for answers to identical questions from ten or more persons other than agencies, instrumentalities, or employees of the United States or for answers to questions from agencies, instrumentalities, or employees of the United States which are to be used for statistical compilations of general public interest. 44 U.S.C. 3502.

Under OMB instructions accompanying the report clearance request form (OMB Standard Form 83), one paragraph is specifically directed to whether sensitive questions may be included and, if so, in what form:

Additional justification must be provided for surveys which include questions of a sensitive nature, such as sex behavior and attitudes, religious beliefs and other matters which are commonly considered private. This should include the reasons why the agency considers the questions necessary and the specific uses to be made of the data obtained. The explanation to be given respondents and any steps to be taken to secure their consent (except where response is mandatory) should be stated. Describe extent of confidentiality and protection provided against disclosure of information from individual returns, including arrangements for disposition of completed report forms. Instructions, III, A-7.

Limitations on Storage, and Dissemination of Information

Limitations on the storage, handling and dissemination of information collected by HEW are found in statutes, Depart-

mental regulations, Civil Service Commission regulations, manuals, policy statements, contract guidelines and miscellaneous memoranda.

The overall Federal government records management policy is set out in 44 U.S.C. 3101 which requires the head of each Federal agency to

...make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities.

As mentioned in the previous discussion of the Federal Reports Act. (pp. 270-271, above) there is a section in that Act discussing when information collected under reports approved under the Act may be released.

(a) If information obtained in confidence by a Federal agency is released by that agency to another Federal agency, all the provisions of law including penalties which relate to the unlawful disclosure of information apply to the officers and employees of the agency to which information is released to the same extent and in the same manner as the provisions apply to the officers and employees of the agency which originally obtained the information. The officers and employees of the agency to which the information is released, in addition, shall be subject to the same provisions of law, including penalties, relating to the unlawful disclosure of information as if the information had been collected directly by that agency.

(b) Information obtained by a Federal agency from a person under this chapter may be released to another Federal agency only—

- (1) in the form of statistical totals or summaries; or
- (2) if the information as supplied by persons to a Federal agency had not, at the time of collection, been declared by that agency or by a superior authority to be confidential; or

(3) when the persons supplying the information consent to the release of it to a second agency by the agency to which the information was originally supplied; or

(4) when the Federal agency to which another Federal agency releases the information has authority to collect the information itself and the authority is supported by legal provision for criminal penalties against persons failing to supply the information. 44 U.S.C. 3508.

Superimposed upon all HEW information disclosure is the Public Information Act, 5 U.S.C. 552. This Act (usually known as the "Freedom of Information Act") establishes a formalized declaration of availability of records and information of all Government agencies. The policy of the Act as implemented in the HEW Public Information Regulation, 45 C.F.R. Part 5, is "...one of the fullest responsible disclosure limited only by the obligations of confidentiality and the administrative necessities recognized by the Act." 45 C.F.R. 5.12. The exemptions from this policy of disclosure which are stated in the Act are:

...matters that are—

- (1) specifically required by Executive order to be kept secret in the interest of the national defense or foreign policy;
- (2) related solely to the internal personnel rules and practices of an agency;
- (3) specifically exempted from disclosure by statute;
- (4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(7) investigatory files compiled for law enforcement purposes except to the extent available by law to a party other than an agency;

(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(9) geological and geophysical information and data, including maps, concerning wells. 5 U.S.C. 552 (b).

The HEW Public Information Regulation provides the operating requirements for the Public Information Act. Whenever certain materials, such as final opinions in the adjudication of cases, which are required to be made available under the Act, relate to an individual, the name or other identifying details shall be removed and the materials shall so indicate, if release of such information would constitute a "clearly unwarranted invasion of privacy." 45 C.F.R. 5.16. The exemptions to required disclosure as set out in the Act are reiterated in the Regulation with amplification of their scope. 45 C.F.R. 5.70 *et seq.* In addition, Appendix A of the Regulation provides examples of exempt materials. Proposed amendments to these regulations take account of experience with the regulations and court decisions. 38 Fed. Reg. 8273, May 30, 1973.

An explicit statutory constraint on disclosure of information which is preserved by exemption (3) is found in section 1106(a) of the Social Security Act, 42 U.S.C. 1306(a), which prohibits disclosure of any personal information obtained by the Department in the course of administration of the Act except as specifically prescribed in regulations issued by the Secretary. (Criminal penalties are provided for violation of this provision.) There are two carefully delimited statutory exceptions from this general prohibition on disclosure of information obtained by HEW under the Social Security Act. The first is Section 1106(c) of the Act which requires the Secretary to furnish an individual's most recent address, or the address of the individual's most recent employer, to a court or a state or local public assistance agency where the individual is sought for purposes of a child support order. 42 U.S.C.

1306(c). See 20 C.F.R. 401.3(g) (3) and (4). The second, found in Section 290(c) of the Immigration and Nationality Act, provides for release of information regarding the identity and location of aliens to any official of the Department of Justice charged with the administration of Title II of that Act. 8 U.S.C. 1360(c). See 20 C.F.R. 401.3(p).

Social Security Administration Regulation No. 1, 20 C.F.R. Part 401, issued under Section 1106 of the Social Security Act, specifies with respect to any information "which in any way relates to, or is necessary to, or is used in or in connection with, the administration of the old-age, survivors, disability, or health insurance programs conducted pursuant to Titles II and XVIII of the Social Security Act," what information may be disclosed, under what circumstances and to whom. (No regulation has been issued to prescribe permissible disclosure of any information obtained by HEW in the course of its administration of the public assistance programs of the Social Security Act, *viz.*, under Titles I, IV, V, X, XI, XIV, XVI, and XIX. Hence, disclosure of such information is barred by Section 1106(a) of the Act.) The disclosures permitted by SSA Regulation No. 1 relate primarily to situations in which: the claimant or his representative gives authorization; disclosure is necessary for a social security program purpose; any official of the Treasury Department or the Department of Justice charged with administration of Titles II, VIII or IX of the Social Security Act, or certain contribution and revenue laws, needs information for the purpose of such administration; any Federal official charged with administration of public assistance, retirement or other benefit payment programs needs information for the purpose of such administration; any State or local agency official charged with administration of various Federally-aided public assistance programs needs information for the purpose of such administration; any authorized Federal official is engaged in investigation or prosecution of a criminal violation of the Act or certain contributions and revenue laws; and the Federal Bureau of Investigation or the U.S. Secret Service is engaged in investigation or prosecution of threat or act of espionage, sabotage or other similar act inimical to national security and certifies in writing that the information requested is required in an investigation of major importance to protect national security. The foregoing and certain other situations when information may be dis-

closed are specified in careful detail in the Regulation. 20 C.F.R. 401.3.

A criminal statute of government-wide applicability provides criminal penalties for unauthorized disclosure of specified classes of information by government officers and employees. This statute states:

Whoever, being an officer or employee of the United States or of any department or agency thereof, publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties or by reason of any examination or investigation made by, or return, report or record made to or filed with, such department or agency or officer or employee thereof, which information concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association; or permits any income return or copy thereof or any book containing any abstract or particulars thereof to be seen or examined by any person except as provided by law; shall be fined not more than \$1,000, or imprisoned not more than one year, or both; and shall be removed from office or employment. 18 U.S.C. 1905.

Its principal focus appears to be the protection of commercial secrets, but the reference to "identity... of any person" and "confidential statistical data" might provide some possibility of employing this statute in cases of unauthorized disclosure of personal data. In any case, however, it merely provides a criminal penalty for disclosing information "in any manner or to any extent not authorized by law." It does not of itself impose an obligation of nondisclosure and does not qualify as a statutory exemption from disclosure under exemption (3) of the Freedom of Information Act (p. 273 above).

Constraints on Grantee Behavior

In some instances HEW's program authority makes explicit statutory provision for the handling of personal information obtained by

HEW grantees. For example, the Social Security Act requires that State plans for the programs of Old Age Assistance, Aid to the Blind, Aid to the Permanently and Totally Disabled, Aid to the Aged, Blind or Disabled, and Medical Assistance for the Aged, provide safeguards which permit the use or disclosure of information concerning applicants or recipients only to public officials who require the information in connection with their official duties, or to other persons for purposes directly connected with the administration of the plan. Social Security Act, § 2(a)(7), 42 U.S.C. 302(a)(7); § 1002(a)(9), 42 U.S.C. 1202(a)(9), § 1402(a)(9), 42 U.S.C. 1352(a)(9); § 1602(a)(7), 42 U.S.C. 1382(a)(7). State plans for Aid to Families with Dependent Children and for Medical Assistance must provide safeguards limiting use or disclosure of information to purposes directly connected with the administration of the plan. Social Security Act, § 402(a)(9), 42 U.S.C. 602(a)(9) and § 1902(a)(7), 42 U.S.C. 139a(a)(7). All the Public Assistance programs of the Social Security Act had, until the Social Security Amendments of 1972 (P.L. 92-603, October 30, 1972) the same limitation on disclosure found in sections 402 and 1902. Those Amendments broadened the access for all the programs except AFDC and Medical Assistance, to permit public officials access to information about applicants and recipients. P.L. 92-603, § 413. The Amendments also provided the broader access in the new program of Grants to States for Services to the Aged, Blind, or Disabled, under a new Title VI which will go into effect on January 1, 1974. § 602(a)(6). The States' obligations with respect to information about recipients in the public assistance programs (other than Medical Assistance) are modified by § 618 of the Revenue Act of 1951, 42 U.S.C. 302 note, which allows States to have legislation allowing access to records of disbursement of public assistance funds as long as the legislation "prohibits the use of any list or names obtained through such access to such records for commercial or political purposes."

HEW implementation of the requirements for safeguarding information is found in 45 C.F.R. 205.50. This regulation is in the process of revision to take account of the 1972 amendments.

The behavior of States in handling information in Public Assistance programs is further constrained by Department instructions on how the States may determine eligibility. Under 45 C.F.R.

206.10(a)(12), a State agency must get the applicant's consent before consulting records about the applicant. Under a recent proposal (37 Fed. Reg. 28189, Dec. 21, 1972), States would have been permitted to consult public records (i.e., records of any public agency, whether or not available for public inspection), without seeking consent. A more recent proposal (38 Fed. Reg. 9819, April 20, 1973) would remove Federal restrictions on State behavior in this area by eliminating from 45 C.F.R. 206.10 any reference to consultation of records. If this proposal is adopted, the resulting flexibility would permit States to consult any records without seeking consent.

Three grant programs in the health field carry their own specific restrictions on grantee handling of patient data. The Venereal Disease Prevention and Control Program under § 318 of the Public Health Service Act, 42 U.S.C. 247c, (added by P.L. 92-449) has a requirement that information about the examination, care, or treatment of any individual carried out under the grant program "shall not, without such individual's consent, be disclosed except as may be necessary to provide service to him. . . ." There is specific provision for disclosure of statistics, or for "clinical or research purposes" as long as the individual's identity is not disclosed.

Two programs under Title XI of the Public Health Service Act provide grants for screening, counseling, and some treatment for sickle cell anemia and Cooley's anemia, two genetic blood disorders. The applicants for the grants "shall— . . . (2) provide for strict confidentiality of all test results, medical records, and other information regarding screening, counseling, or treatment of any person treated, except for (A) such information as the patient (or his guardian) consents to be released, or (B) statistical data compiled without reference to the identity of any such patient. . . , § 1104(a)(2) and § 1113(a)(2) of the Public Health Service Act; 42 U.S.C. 300b-3(a)(2) and 300c-2(a)(2).

The Social Security Amendments of 1972 added a new Part B to Title XI of the Social Security Act. This authorizes the Secretary to enter into agreements with organizations to review, from a technical and professional standpoint, the necessity and quality of medical services for which payment may be made under the Social Security Act. (This includes Medicare, Medicaid, and certain child health programs.) These organizations will be nonprofit associations of physicians, or other organizations found able to perform the task, and are designated Professional Standards Review Organizations.

Certain obligations with respect to confidentiality are imposed by the statute. Under § 1155(a)(4), 42 U.S.C. 1320c-4(a)(4), these organizations must arrange for the maintenance and review of

profiles of care and services received and provided with respect to patients, utilizing to the greatest extent practicable in such patient profiles, methods of coding which will provide maximum confidentiality as to patient identity and assure objective evaluation consistent with the purposes of this part.

There is a prohibition on disclosure of information in § 1166, 42 U.S.C. 1320c-15, which is somewhat similar to the one in § 1106. Under § 1166, data or information acquired by any Professional Standards Review Organization shall be held in confidence and not disclosed except as necessary to carry out the purposes of the program, or under "such circumstances as the Secretary shall by regulations provide to assure adequate protection of the rights and interests of patients, health care practitioners, or providers of health care." Fine, imprisonment, and the costs of prosecution are provided as penalties.

Section 305(a) of the Public Health Service Act authorizing the Secretary to conduct the National Health Surveys and Studies, 42 U.S.C. 242C (pp. 263-264, above) includes the following constraint added by P.L. 91-515:

No information obtained in accordance with this paragraph may be used for any purpose other than the statistical purposes for which it was supplied except pursuant to regulations of the Secretary; nor may any such information be published if the particular establishment or person supplying it is identifiable except with the consent of such establishment or person.

Explicit provision to authorize constraints on disclosure of personal information in research relating to drugs is found in § 303(a) of the Public Health Service Act, 42 U.S.C. 242a, as follows:

The Secretary may authorize persons engaged in research on the use and effect of drugs to protect the privacy of individuals who are the subject of such research by withholding from all persons not connected with the conduct of such research the names or other identifying characteristics of such individuals. Persons so authorized to protect the privacy of

such individuals may not be compelled in any Federal, State, or local civil, criminal, administrative, legislative, or other proceedings to identify such individuals. 42 U.S.C. 242a.

Similar authority with respect to alcohol research is found in § 333 of the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970. 42 U.S.C. 4582. The Attorney General has similar authority with respect to drug research under § 502(c) of the Comprehensive Drug Abuse Prevention and Control Act of 1970, 21 U.S.C. 872(c). In these authorities, the authorization to hold data confidential may be given to anyone conducting the specified research; there is no requirement of Federal connection. The authorization with respect to drug research has been given to Federal employees not in HEW and to employees of an OEO-funded project with no HEW connection, 37 Fed. Reg. 21547, Oct. 12, 1972, and to employees of HEW contractors doing alcoholism research. 37 Fed. Reg. 28310, Dec. 22, 1972.

Availability of Public Health Service records and information is governed by 42 C.F.R., Part 1. Clinical information as defined is confidential and is available "...only as necessary for the performance of the functions of the Service" or in certain limited instances, such as to a patient or his designee upon a reasonable showing of need; to a government agency which requested or arranged for examination, care or treatment service facilities; or to State or public health agencies "engaged in collecting data regarding disease." 42 C.F.R. 1.102. In addition, upon a court order, clinical information shall be disclosed in accordance with applicable local law regarding confidentiality of physician-patient communications.

When non-clinical information has been obtained under an assurance of confidentiality, it may be disclosed only with the consent of the person or agency to whom the assurance was given or when the Secretary determines that disclosure is necessary to prevent "an epidemic or other grave danger to the public health" or in a legal action brought against the Government. 42 C.F.R. 1.103.

The regulations contain additional limitations on release of records and information concerning actions of advisory councils; regulatory programs such as licensing of biological products; conduct of research projects; and applications for employment or Federal support.

Six other regulations provide limitations on dissemination of information.

42 C.F.R. 200.12 provides that State Plans for maternal and child health and crippled children's programs shall provide for designation of all personal information as confidential with suitable regulations and safeguards to be provided. However, information which does not identify particular individuals may be disclosed in summary or statistical form.

42 C.F.R., Part 3 provides, among other conditions, that the Special Statistical Services of the National Center for Health Statistics may be furnished provided that "the data or statistics requested are not confidential."

42 C.F.R., Part 300 provides that the records of Saint Elizabeth's Hospital are confidential and may be disclosed only upon a court order or if the Superintendent determines that it would "not be inimical to the public interest or to the welfare of the patient." 42 C.F.R. 300.2.

21 C.F.R., Part 4 provides for procedures to be followed by persons desiring to obtain records and information of the Food and Drug Administration not specifically available under the Freedom of Information Act and the Department's implementing regulations.

The Food and Drug Administration (FDA) regulation governing investigational new drugs and approved new drugs specifically provides that the identity of individual patients need not be divulged by a clinical investigator physician unless the records of particular subjects require a more detailed study by FDA personnel of the case history or unless there is reason to believe that the records do not represent actual cases studied or do not represent actual results obtained. 21 C.F.R. 130.3(a)(12), 130.3(a)(13), and 130.13(c).

Disclosure of individual information obtained in the administration of the Social and Rehabilitation Service repatriation assistance program, authorized by Section 1113 of the Social Security Act, 42 U.S.C. 1313, is carefully constrained by regulation for the benefit of assisted individuals. 45 C.F.R. 212.9.

Other Limitations

In addition to the statutes and regulations discussed above, guidelines relating to disclosure of information exist in many other forms including manuals, circulars and instructions, policy statements, contract clauses, and assurances on data collection forms. Many of

these develop and enlarge upon the policies and procedures which are prescribed in statutes and regulations. In other instances, these guidelines have been promulgated in the absence of any specific statutory or regulatory provisions. Examples of such guidelines are as follows.

The National Center for Health Statistics (NCHS) has issued a comprehensive policy statement on release of data. Simply stated, this policy is one of "absolute and uncompromising protection of confidentiality. . .with respect to data supplied by respondents as privileged communications." Data are never to be released in a manner in which a respondent's identity is revealed, but rather only as aggregate statistics. Detailed procedures for handling particular classes of data or programs are provided. Furthermore, there are restrictions placed on the use of the statistics themselves so that there will be no misuse or misrepresentation. The NCHS requires a pledge in each contract that confidentiality of records will be maintained and that access to data will be strictly limited. A document signed by Surgeon General L.E. Burney on February 26, 1957 and published in the Federal Register, 22 Fed. Reg. 1687 (March 15, 1957), underscores the guarantees. This is supplemented by another similar assurance published in May, 1959. 24 Fed. Reg. 4061 (May 20, 1959). Furthermore, most data collecting questionnaires carry a confidentiality assurance. All persons engaged in data-collecting activities with NCHS must also sign an affidavit guaranteeing non-disclosure.

Health Services and Mental Health Administration Circular No. 71.1 entitled, "Assurances of Confidentiality Given in Obtaining Information" sets out the Public Health Service policy for the Health Services and Mental Health Administration (HSMHA) governing when such assurances shall be given, what form the assurance shall take and what the responsibilities are with respect to information collected subject to the assurance.

In situations where information is collected and stored by third parties under contracts with HEW, generally either the contracts themselves or contract guidelines include confidentiality provisions. The Community Care Contract Agency Series, guidelines prepared by the Narcotic Addict Rehabilitation Branch of the National Institute of Mental Health, provide that the records maintained for each patient will be kept confidential and that release of information,

other than to government program personnel and the Federal courts, will be permitted only with the patient's signed consent.

Social Security Administration (SSA) contracts with intermediaries and carriers, e.g., Blue Cross, include clauses directing them to adopt policies and procedures to insure that information obtained in carrying out their functions under the Social Security Act shall be used and disclosed solely as provided in SSA Regulation No. 1 (p. 275, above). Furthermore, the contractors must agree to include in all subcontracts disclosure clauses identical to those in their own contracts.

The Social Security Claims Manual, SSA's operating instructions for its employees, contains an entire chapter devoted to disclosure of information. See Ch. 7300. This chapter, is keyed to the regulations, 20 C.F.R., Part 401, and covers in rigorous detail, circumstances under which disclosure is allowed.

The Social Security Handbook, which does not have the force of law, contains nine pages bearing directly upon the subject of what information SSA may or may not disclose under specified conditions and circumstances. Handbook, §§ 141-153 and 1701. The Handbook was published to provide a detailed explanation of the social security program to the public and it does not reflect changes in the regulations since early 1968.

A guide to policies governing the provision of special statistical information, records, and related materials created pursuant to Section 417 of the General Education Provisions Act, 20 U.S.C. 1231f (p. 262, above), was adopted by the Office of Education in March, 1972. 37 Fed. Reg. 6218 (March 25, 1972). The basic policy is "to make. . .collected statistical information available. . .as widely and promptly as possible" subject to certain constraints including non-violation of confidentiality of data.

Permanent Storage and Disposal of Information

A comprehensive statutory scheme vests authority for management of Federal government records in the General Services Administration (GSA) including generally supervising each agency's record keeping, setting standards for selective retention of records, establishing centers for storage, processing and servicing of records, and finally, regulating and handling the ultimate disposal or permanent

storage of all government records. 44 U.S.C. 2901-2910 and 44 U.S.C. 3301-3314.

Records that contain information that is subject to confidentiality restrictions remain subject to such protection when transferred to GSA, as provided by a regulation that states:

Whenever any records that are transferred are subject to restrictions upon their use, imposed pursuant to statute, Executive order, or agency determination, such restrictions shall continue in effect after the transfer. Restrictions imposed by agency determination may be removed by agreement between the agencies concerned. 41 C.F.R. 101-11.409-8.

Personnel Information Activities

In addition to the authority to collect personnel information to fulfill general Departmental administrative responsibilities (pp. 260-261, above), there is a duty imposed upon the Department to collect personnel information to fulfill Civil Service Commission (CSC) requirements. Under the provisions of 5 U.S.C. 2951 and Executive Order 10577, HEW is required periodically to provide various personnel-related reports to the Civil Service Commission. Section 7.2 of Civil Service Rule VII provides that:

Each agency shall report to the Commission, in such manner and at such times as the Commission may prescribe, such personnel information as it may request relating to positions and officers and employees in the competitive service and in the excepted service, whether permanent or career, career-conditional, indefinite, temporary, emergency, or subject to contract. 5 C.F.R. 7.2.

The data required for these reports are essentially those supplied on the CSC Standard Form 50, Notification of Personnel Action. That information consists of basic personal data (name, sex, birth date); basic employment data (grade, dates of entrance into service and of potential promotion, pay plan and occupation code, insurance codes, type of personnel actions taken); veteran preference code and handicap code. See Federal Personnel Manual, Chapter 291.

Civil Service Commission regulations deal extensively with the maintenance of personnel records. The regulations require establishment of an Official Personnel Folder for each employee, 5 C.F.R. 293.202, which Folder is under the jurisdiction and control of and part of the records of the Civil Service Commission. 5 C.F.R. 293.203. In these Folders each agency is obliged to maintain reports of selection and other personnel actions as listed in 5 U.S.C. 2951 and also other records as required by Commission instructions. 5 C.F.R. 293.204. There is a provision relative to removal of records of only temporary value from the Folder. 5 C.F.R. 293.209.

Another requirement for collection of information about Federal employees is found in 5 C.F.R. 713.302 which calls for periodic reporting of employment statistics by race and national origin. CSC regulations provide that data as to race or national origin may be collected only by visual identification. 5 C.F.R. 713.302(b). In addition, anyone having the authority to take or recommend personnel action in the competitive service is prohibited from making any inquiry concerning race, religion, or political affiliation of any employee in, or any eligible or applicant for, the competitive service. 5 C.F.R. 4.2.

The disclosure of information collected for personnel purposes is limited by statutes and regulations as follows. The Freedom of Information Act specifically exempts from public disclosure matters

related solely to the internal personal rules and practices of an agency. . . .[and] personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. 5 U.S.C. 552(b)(2) and (6).

These sections are amplified in regulations of both the Civil Service Commission, 5 C.F.R. 294.103, and the Department, 45 C.F.R. 5.72 and 5.76 (p. 274, above).

The general policy of the Civil Service Commission is to make information available unless disclosure would constitute a clearly unwarranted invasion of personal privacy or is otherwise prohibited by law. Medical information may not be made available without the individual's written consent, 5 C.F.R. 294.401, nor may informa-

tion from annual and sick leave records, 5 C.F.R. 294.1101. Names, present and past positions, titles, grades, salaries and duty stations of government employees are publicly available, except when release of such information is prohibited by law or Executive order or when the information is sought for commercial or other solicitation or for political purposes. Employee's name, address, Social Security number, and amount of Federal compensation are furnished to State or local taxing authorities pursuant to Office of Management and Budget Circular No. A-38, Revised. In addition, limited information may be made available to prospective employers and home address shall be made available to a police or court official for the purpose of service of a summons, warrant, subpoena or other legal process. Approved educational and historical researchers may be granted limited access to information about separated employees which is stored with the General Services Administration; however, information that is derogatory to the former employee shall not be made available under this provision. 5 C.F.R. 294.702. With the exception of certain medical information, test material, and investigative reports, employees, former employees, and their representatives or other persons having their consent may have access to their Official Personnel Folders. Finally, Official Personnel Folders are, with limitations on material relating to loyalty and security, officially accessible to members of Congress, representatives of Congressional committees and subcommittees, government officials of the District of Columbia and Federal executive branch officials. 5 C.F.R. 294.703. Provision exists for limited disclosure to the parties concerned and to the public of information from administrative appeal and complaint files established for purposes of employee grievances and administrative appeals. 5 C.F.R. 294.801.

Instructions, letters and bulletins are issued by the Civil Service Commission periodically to amplify, update, and reinforce the requirements provided in statutes and regulations. The instructions of the Civil Service Commission, found in the Federal Personal Manual (FPM), are issued under the authority of Executive Order 10561 and under the regulations discussed above. They apply to all executive departments and agencies. Chapter 290 of the FPM, added in 1969, is designed to guide agencies in the use of automated data processing in personnel administration. It discusses modifications of standard forms necessary or desirable when automated processing is

used and also lists data elements necessary to meet reporting requirements, FPM, Ch. 290, Appendix A, and mandatory and optional data elements when an automated system is used. FPM, Ch. 290, Appendix B.

Appendix H

Mailing Lists

DANIEL H. LUFKIN*

I would to God thou and I knew where a commodity of good names were to be bought.

—Falstaff
Henry IV, Part I, I, ii.

If Falstaff had waited five hundred years, he would have had no difficulty at all in buying all the names he wanted, for names, like any other commodity, are bought, sold, rented, and traded in the lively, mercurial industry of direct-mail advertising. Probably no other application of electronic data processing has had a broader effect upon so large a population as the headlong computerization of the mailing list. The United States Postal Service handles slightly more than one piece of mail per day for every man, woman, and child in the country. About a quarter of the volume moves as third-class matter; i.e., printed material that is neither a periodical nor a book. In practice, nearly all third-class mail is advertising or appeals for funds.

*Staff Consultant to the Committee

Since its origin a century ago, the direct-mail industry has grown to represent an advertising expenditure of about \$3 billion per year, or about one-seventh of the total national advertising volume. Mail advertising moves about \$50 billion annually in goods and services, or roughly 5 percent of the Gross National Product. Divided among the 260,000 holders of Postal Service bulk third-class permits, this represents an average annual volume of business of about \$200,000 per holder. A Department of Commerce estimate that only a tenth of all permit holders have more than 100 employees, and only half have more than 10, supports the industry's contention that it is dominated, numerically at least, by small firms operating locally. The largest single class of mailings, accounting for slightly less than 10 percent of the total, is magazine subscription offers.

Although direct-mail advertising is one of the more common experiences of everyday life, public attitudes toward it are studded with inconsistencies and contradictions, likely reflecting the fact that few people give it much thought one way or the other until they are asked a specific question by an interviewer. Even then, the dissonance of being intruded upon by a survey on privacy may well distort the replies. In privacy-minded Britain, for example, only about 2 percent of the respondents in the Younger Committee's survey spontaneously mentioned that their privacy had been invaded through the mail, and much of that response was apparently prompted by recent (1970) saturation mailings advertising sex manuals and the *Reader's Digest* (in separate mailings, of course).¹ In the United States, a Nielson survey found that 87 percent had no objection to being addressed as "occupant".² In a survey on behalf of the American Federation of Information Processing Societies (AFIPS), however, 63 percent of the respondents voted for a decrease in "using computers to send mail advertisements to the home," and 84 percent felt that the Government should be concerned with that use.³

¹ *Report of the Committee on Privacy*, Rt. Hon. Kenneth Younger, Chairman, (London: H. M. Stationery Office), 1972, pp. 123, 125-127.

² *Factsheet: Direct Mail Advertising* (New York: Direct Mail Advertising Association), 1973, p. 2.

³ American Federation of Information Processing Societies and TIME magazine, *A National Survey of the Public's Attitudes Toward Computers* (New York: AFIPS-TIME, Inc.), 1971. The summary is discussed in Alan F. Westin and Michael A. Baker, *Databanks in a Free Society* (New York: Quadrangle Books), 1972, pp. 481-484.

Since privacy, like happiness, is essentially a subjective state, it is not easy to frame the arguments against direct-mail advertising in legal or procedural terms. The arrival of the mail itself is scarcely an intrusion, since one is free to throw it away unread. The argument on the simple ground of annoyance has not been upheld by the courts.

The mail box, however noxious its advertising contents often seem to judges as well as other people, is hardly the kind of enclave that requires constitutional defense to protect "the privacies of life!"⁴

Iago's claim of "He that filches from me my good name Robs me of that which not enriches him And makes me poor indeed,"⁵ is popular but fails on the grounds that one's name is not ordinarily damaged by use in a mailing list and that the use does indeed enrich the lister.

In those exceptional cases in which the name does suffer damage because the character of the mailing holds the addressee in a false light, as when sexually oriented matter fails to arrive in a plain brown wrapper, the common law does afford the addressee the same rights of action as in any other case of defamation. A Federal statute furthermore allows a person to specify in advance of any intrusion that he does not wish to receive sexually oriented advertisements through the mail.⁶

An individual who desires to avoid receiving sexually oriented mail advertising fills out and submits a Postal Service Form 2201. Each adult of 19 or over must submit a separate form, but a parent may list up to four children on his own form. These forms are processed at Postal Service headquarters and prepared in list format as both magnetic tape and printed copy. The lists are made available for sale to firms that carry on sexually oriented advertising. The law provides a penalty for mailing such advertising to any person who has been on the Postal Service list for more than 30 days. (Note that this service would be practically impossible to administer without the use of a computer to compile the list and keep it up to

⁴ *Lamont v. Commissioner of Motor Vehicles*, 269 Fed. Supp. 880, 883 (S.D.N.Y. 1967).

⁵ *Othello*, III, iii.

⁶ 39 U.S.C. 3010-11.

date.) The onus of deciding whether a given advertisement is sexually oriented is put on the advertiser, who, if he has any doubt at all, is unlikely to risk a mailing when he knows that the chance of a sale is practically nil, and that he risks criminal prosecution if a recipient whose name is listed considers the advertisement objectionable.

Another, earlier, statute provides a means for an individual addressee to obtain a Postal Service order (i) prohibiting any particular mailer from sending him advertisements that the addressee, in his sole discretion, believes to be "erotically arousing or sexually provocative," (ii) directing the mailer to delete the addressee's name from all mailing lists owned or controlled by the mailer, and (iii) prohibiting the mailer from the sale, rental, exchange, or other transaction involving mailing lists bearing the addressee's name.⁷

The Direct Mail Advertising Association, Inc., the industry's largest trade organization, also makes a list of people who want to be removed from mailing lists. Since the Association excludes mailers of sexually oriented material from membership, its de-listing service is meant to affect ordinary commercial and charitable lists. Forms for taking advantage of the Association's "Mail Preference Service" are available from its headquarters at 230 Park Avenue, New York, New York 10017. According to the DMAA, a consolidated listing of those who "wish to get out of the mail mainstream" is distributed monthly to its approximately 1,600 members. Although the Association points out that no particular sanctions apply to the Mail Preference Service listings, most advertisers are glad to remove nonproductive names, since "cleaning" increases the trading and rental value of their lists. In fact, most mailers will cheerfully remove a name from a list, if the list they are using happens to be under their own control and not merely rented from a broker. Most mailers, DMAA members and independents both, find that requests to be removed from the lists average 3 or 4 persons per 10 thousand addressees per year.

If getting off a list takes initiative and a degree of sophistication, getting on the list in the first place is so easy as to be practically inevitable for most people. To begin with, both the Direct Mail Advertising Association and a number of independent brokers oper-

⁷ 39 U.S.C. 3008.

ate enlisting services. The Association's operation lends a symmetry to the Mail Preference Service by providing a form to get *on* mailing lists in any of 22 different categories. The independents usually place modest classified ads in popular magazines: "Receive BIG mails. Your name on 50 lists, 50 cents". As one might expect, lists compiled from this source include mostly curious teen-agers. Most persons join the lists through more indirect, but nonetheless effective, paths.

Almost any action that puts a name and its associated address into the hands of a commercial or service organization will put that name on a mailing list—subscribing to a magazine, buying an item by mail from a magazine advertisement, buying air-travel insurance at an airport, joining a professional or scientific society, donating to a charity or a political campaign, returning the warranty card from a purchase, holding a credit card, or taking out a mortgage. In many cases, registering a car, getting born or married, going to school (public or private), being in the telephone directory, or qualifying for a license as a driver, pilot, or riverboat master will provide all the record an entrepreneur needs to add a name to his list.⁸

It is this industry practice of compiling lists from official records that seems to generate the most consistent opposition to the mailing-list industry. However, since administrative records are presumed to be public unless otherwise designated, and since openness of records serves well-recognized democratic ends, it seems an unnecessarily Procrustean solution to restrict access to public records merely to make life more complicated for advertisers. In fact, competitive pressure often forces commercial list agencies to abandon public records as too outdated and to develop other sources for the same data. Birth records in many jurisdictions, for example, often lag as much as 60 days, so that the psychological edge of a fine-honed mailing to sell insurance to the new father, for instance, would be badly dulled. Most commercial birth lists are compiled from private agreements with hospitals (or with hospital employees), newspaper birth announcements, or from orders with diaper services or dairies. Some of the larger lists, particularly for

urban areas, are derived from city directories (themselves the product of a private census effort by the R. L. Polk organization), or from the telephone book.

Starting with a raw list of names and addresses from the telephone book, for example, a listing organization may sort the addresses by census tract for a first cut at arranging the list by income. Census tracts, the smallest units for which decennial census data are regularly published, cover urban neighborhoods of about a thousand families each. For each tract population, the census reports median income and education, average family size, distribution of occupations, size and type of housing, and other statistical data that permit a fairly accurate estimate (American neighborhoods being as homogeneous as they are) of the buying power of every individual on the raw telephone-book list.

So far, making the list has demanded only modest clerical resources. Although most telephone books are computer-produced to begin with, and thus already exist in machine-accessible form, a good deal of handwork is required to sort out listings that do not conform to the usual structure of names. (Despite the earnest efforts of mailers and their computer experts, there is a whole class of computer stories about the Little Sisters of the Poor, for instance, getting offers beginning "Dear Mrs. Little.") In some towns, this handwork is the basis for a sizeable cottage industry.

Other useful sources of names are the rosters of various license holders and professional societies. Lists from these sources allow highly selective mailings to advertise specialized books and equipment. Since most recipients are genuinely interested in the advertised matter, there is little opposition to direct mail from this source, although clubs of stamp and coin collectors take pains to protect their members from inadvertently advertising their collections to burglars.

With lists of various sorts to work from, relatively simple computing equipment will enable a list broker to assemble very specialized mailings. Matching a medical society list against census tract addresses against motor vehicle registrations, for example, can easily produce a list of physicians in a given suburb who own Oldsmobiles more than two years old. A sales message tuned to just that audience may have excellent results.

⁸ See *Sale or Distribution of Mailing Lists by Federal Agencies*, Hearings before the Subcommittee on Foreign Operations and Government Information of the Committee on Government Operations, U.S. House of Representatives, 92nd Congress, 2d Session, June 13 and 15, 1972 (Washington, D.C.: U.S. Government Printing Office), 1972.

In some cases, the computer can be used to generate specialized lists from a single mass list like the telephone book. A simple program can print out all addresses for which more than one family name is listed to produce a list of apartment-house dwellers. The computer may simply replace every name on the list with the word "occupant," trading the benefits of a personalized approach for those of easier postal delivery. Computer programs are even available which will sort names into ethnic categories. These claim accuracies of better than 75 percent and have been widely used in recent political campaigns.

There is some evidence, however, that this selective computer-tuning of advertising may have passed its peak of popularity. In part, this may be due to rising concern about personal privacy, but it is also likely that the computer-written letter has itself lost some of its novelty. Whatever the reason, except for the very largest direct-mail firms, mostly magazines, there are few companies that find extensive computer work in fine-tuning mailing lists worth the expense of a special automated facility. The managers of the small and middle-sized firms that account for the bulk of direct-mail advertising usually prefer to work from "fresh" lists of people who have recently bought merchandise through the mails. A list may well have originated from a completely different kind of product or service (in fact, direct competitors usually do not exchange lists and even "salt" their own lists with the names of friends who will watch their mail for unauthorized use), but freshness and accuracy of addresses are considered more valuable than affinity. Since about 20 percent of the U.S. population changes address each year, the useful life of any list is ephemeral. Unless the fixed costs of the computer operation can be shared with payroll, inventory, and other conventional business tasks, sophisticated computer processing of mailing lists is not economically practical for most firms.

To what extent should the safeguards suggested by the Secretary's Advisory Committee on Automated Personal Data Systems apply to the direct-mail industry? We have found no evidence that direct-mail advertising is anything more than an annoyance to a small part of the population. That small part, however, deserves its share of reasonable protection. Furthermore, there is no way of knowing whether the number of annoyed people today will grow as an increase in computer-tuned mailing begins to vex those who are

now neutral about it. Certainly it should be easier to deal with such an eventuality if pains are taken now to understand the present situation.

An underlying function of the Advisory Committee's recommended safeguards is to provide effective feedback mechanisms that will help to make automated personal data systems more responsive to the interests of individuals. Systems maintained by most government agencies, and by many private organizations, do not now provide for tight links between individuals and the system operators. The direct-mail industry, however, is largely organized around the idea of public feedback; the trade press concentrates almost obsessively on methods for maximizing response and minimizing complaints.

Because most mailings draw a response from only 3 or 4 percent of the addressees, a small change in the response rate can have relatively large economic implications for the mailer. The same is true for the compilers and brokers of mailing lists, because the price a list commands in the rental market depends not so much on its demographic sophistication as on its accuracy and freshness. Lists are cleaned by adding a special imprint to the mailing which gives the Postal Service authority to correct and return (at first-class rates) all undeliverable pieces. Since it costs about four times as much to discover and correct a "nixie" as it does to make a clean mailing in the first place, there is a powerful economic incentive to concentrate lists on known buyers at addresses of known accuracy.

Another feedback mechanism operates on the industry as a whole. Direct-mail advertising is strongly dependent for survival on the official good will of a large number of agencies of the government; opposition from the Postal Service, from motor vehicle registrars, or from the Census Bureau, to name a few examples, would seriously hamper the industry on its present scale. It seems likely that a scandal involving public records, or the development of a public allergy to direct-mail advertising, would lead to government moves to put constraints on the industry.

Constructive publicity toward emphasizing the rights of the individual relative to direct-mail advertising, especially the methods the industry has adopted for getting off and getting on the larger lists, would go far in strengthening these feedback mechanisms that already operate. In particular, the Direct Mail Advertising Associ-

ation's Mail Preference Service deserves wider attention. Although the Association claims that the service has received wide publicity throughout the country, it does not seem to have made a very deep impression on the public mind. This may reflect the persistent antagonism between the direct-mail industry and newspapers and magazines. Competition for the advertising dollar has often led periodicals to adopt a jaundiced editorial view of "junk mail," and it may therefore be that the Mail Preference Service will have to be publicized mainly through official, especially Postal Service, channels.

If feedback mechanisms stronger than those provided by the economics of the industry should become desirable, there would be formidable practical difficulties in applying the Committee's safeguards to the freewheeling small operators of the direct-mail industry. The most directly applicable of the Committee's safeguards is the requirement for the informed consent of the data subject to be obtained before any collateral use may be made of data from an administrative personal data system. To accomplish this, forms that are used by the system in transactions with individuals (applications, for example), and that are vulnerable to mailing-list uses, could be printed with a block in which the individual—by his deliberate action—could indicate whether or not his name and address could be sold or otherwise transferred to another data system for mailing-list use. Of course, this could not prevent his name and address from being copied by hand out of a public record system, but the cost of such handcopying would sharply curtail much commercial use.

In view of the controls already at work in the direct-mail advertising industry, this limited application of the Committee's safeguards seems sufficient. It would provide protection to individuals from having their names unexpectedly appear on mailing lists without their consent. We doubt the utility and feasibility of trying to make the rest of the Committee's proposed safeguard requirements apply to mailing lists as such, as a form of administrative automated personal data system, or to organizations that deal only in mailing lists. If the control of mailing lists is to be undertaken by law, it should be done by legislation that is directed specifically to that purpose. Any attempt to do so by less direct means, such as through the application of all the Committee's safeguards, would be likely to prove ineffectual, unless the courts come to place a value

on mailbox privacy far higher than that reflected in the *Lamont* case cited earlier.⁹ Long before that would have occurred, popular feeling against intrusion on personal privacy would have had to rise to such a pitch that the direct-mail business would already have become, for the first time, flat, dull, stale, and unprofitable.

If the foregoing analysis of the situation underestimates the felt need for greater mailbox privacy, it would be feasible to undertake specific legislative action against the direct-mail advertising industry to provide greater protections, as the regulation of information practices in the consumer-reporting industry amply demonstrates.

⁹Note 4, p. 290, above.

Appendix I

Bibliography on Record Keeping and Personal Privacy

Acheson, E.D. *Medical Record Linkage*. London: Oxford University Press, 1967.

Advisory Committee on Problems of Census Enumeration. *America's Uncounted People*, edited by Carole W. Parsons. Washington, D.C.: National Academy of Sciences, 1972.

The report of a committee funded by the Bureau of the Census, the Manpower Administration of the Department of Labor, and the Office of Economic Opportunity. Chapter 1 examines some of the public policy implications of inadequate social statistics. Chapters 4 and 5 outline a strategy for research on people who are not included in censuses and social surveys.

Aitken, Jonathan. *Officially Secret*. London: Weidenfeld and Nicolson, 1971.

An account of the trial and acquittal of the author who was prosecuted for alleged violation of the Official Secrets Act (1911). Six chapters are devoted to the history of the Official Secrets Act in Great Britain. In the final chapter, the author argues for radical reform of the Act and discusses various legislative alternatives.

American Anthropological Association. "Principles of Professional Responsibility." Adopted by the Council of the American Anthropological Association, Washington, D.C., May 1971.

American Association for Public Opinion Research. "Code of Professional Ethics and Practices." New York: American Association for Public Opinion Research, 1970.

American Bar Association. Standing Committee on Law and Technology. *Computers and the Law*, edited by Robert P. Bigelow. 2nd ed. New York: Commerce Clearinghouse, Inc., 1969.

Lists the uses of computers by lawyers. See especially, Richard I. Miller, "Data Banks and Privacy;" Lee Loevinger, "Federal Regulation of Computers," on the regulation of computer communications; and "Law Enforcement and Criminal Justice," which includes a list of computer-based criminal justice information systems.

American Civil Liberties Union. *Policy Guide*. New York: American Civil Liberties Union, 1967.

American Council on Education. Office of Research. *Users' Manual: ACE Higher Education Data Bank*. ACE Research Reports, 4:1, 1969.

American Hospital Association. "Statement on a Patient's Bill of Rights." Chicago: American Hospital Association, November 17, 1972.

American Institutes for Research. *The Project TALENT Data Bank: A Handbook*. Palo Alto, Calif.: American Institutes for Research, 1972.

American Justice Institute. Correctional Decisions Information Project. 6 vols. Sacramento, Calif.: American Justice Institute, 1972.

Vol. 1: Correctionetics: Modular Approach to an Advanced Correctional Information System

Vol. 2: Appendix A: Program Narratives and Flow Diagrams
Appendix B: List of Case Events

Vol. 3: Appendix C: Offender Data File

Vol. 4: Appendix D: Description of a Computer-Based Simulation of a Correctional Management Information System
Appendix E: Pilot Study of the Use of Data in Case Decision-Making in Corrections

Vol. 5: Appendix F: A Plan for the Development and Operation of a Job Matching System for the California Department of Corrections

Vol. 6: Appendix G: Management Display Center Operation and Training Manual

American National Standards Institute. *ANSI Standard: Identification of Individuals for Information Interchange*. New York: American National Standards Institute, 1969.

American Psychiatric Association. "Position Statement on the Need for Preserving Confidentiality of Medical Records in Any Health Care System." *American Journal of Psychiatry*, 128:10 (April 1972), 169.

Recommendations of the American Psychiatric Association's Task Force on Confidentiality as It Relates to Third Parties.

_____. Task Force on Automation and Data Processing in Psychiatry. *Task Force Report*. Washington, D.C.: American Psychiatric Association, 1971.

Examines the use of computers in ten areas related to the practice of psychiatry. For discussions of confidentiality, ethics, and legality, see sections on data analysis, data banks, automated clinical records, and assessment and treatment techniques.

American Psychological Association. Ad Hoc Committee on Ethical Standards in Psychological Research. *Ethical Principles in the Conduct of Research With Human Participants*. Washington, D.C.: American Psychological Association, 1973.

American Sociological Association. Committee on Information Technology and Privacy. "Report of the Committee on Information Technology and Privacy." *American Sociologist*, 5:4 (November 1970), 409-411.

American Statistical Association. "Maintaining the Professional Integrity of Federal Statistics: A Report of the American Statistical Association - Federal Statistics Users Conference Committee on the Integrity of Federal Statistics." *The American Statistician*, 27:2 (April 1973), 58-67.

Anderson, Ronald E. "Sociological Analysis of Public Attitudes Toward Computers and Information Files." *American Federation of Information Processing Societies Proceedings: Spring Joint Computer Conference*, 40 (Spring 1972), 649-657.

Anderson, Stanley V., and Glen McKay. "A List of Law Journal Articles, Comments and Notes on the Federal Freedom of Information Act." Ombudsman Activities Project, University of California at Santa Barbara, September 1972.

A guide to approximately 40 articles that appeared in journals between 1957 and 1970.

Anderson, Wayne, and Steve Sherr. "Confidentiality Expectations of College Students: Revisited." *The Journal of College Student Personnel*, 10:4, July 1969, 264-269.

A survey reveals attitudes of college students pertaining to the release of information held by the school administration. Students discriminated between yes/divulge and no/retain according to the type of information, the recipient person or agency, and specific or blanket release practices.

Arnold, Joanne E. *Full Disclosure: New and Responsible Attitudes*. Boulder, Colorado: National Center for Higher Education Management Systems at Western Interstate Commission for Higher Education, 1972.

On how much of the conduct of public affairs should be public information.

Aronoff, Stanley J. "1984—Only 11 Years Away." *State Government*, 46:2 (Spring 1973), 66-75.

Association of Computer Programmers and Analysts. "The Data Bank and Your Privacy: The ACPA's Position." *ACPA: The Newsletter of the Association of Computer Programmers and Analysts*, September-October 1972, 3-6.

Association of Data Processing Service Organizations, Inc. "ADAPSO's Position Paper on Privacy Problems." News Release, New York, October 21, 1970.

Astin, Alexander W., and Robert F. Boruch. "A 'Link' System for Assuring Confidentiality of Research Data in Longitudinal Studies," *American Educational Research Journal*, 7:4 (November 1970), 615-624.

Bancroft, T. A. "The Statistical Community and the Protection of Privacy." *The American Statistician*, 26:4 (October 1972), 13-16.

Comments on the proposed National Data Center and the recommendations for protecting the confidentiality of personal data in *Federal Statistics*, Report of the President's Commission on Federal Statistics, Vol. 1.

Behavioral and Social Sciences Survey Committee. *The Behavioral and Social Sciences: Outlook and Needs*. A report prepared under the auspices of the Committee on Science and Public Policy (National Academy of Sciences) and the Committee on Problems and Policy (Social Science Research Council). Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1969.

The report recommends that "a special commission be established to investigate in detail the procedural and technical problems involved in devising a national data system designed for social scientific purposes; that it recommend solutions for these problems and propose methods for managing a system that will make data maximally useful, while protecting the anonymity of individuals."

Bigelow, Robert P., ed. *Computer Law Service*. Chicago: Callaghan & Company, 1972.

"The purpose of the *Computer Law Service* is to provide the practicing lawyer with explanatory articles, reference materials and the decisions of courts and agencies that will help him handle the legal problems that have been raised by the invention and use of the computer."

Bisco, Ralph L., ed. *Data Bases, Computers and the Social Sciences*. Information Sciences Series. New York: Wiley-Interscience, 1970.

A selection of papers from the Conference of the Council of Social Science Data Archives at UCLA in June 1967. For a discussion of computerized

information systems in government, see Raymond T. Bowman, "The Idea of a Federal Statistical Data Center—Its Purposes and Structure;" and Roye L. Lowry, "Federal Information Systems—Some Current Developments." See also Part III, "Studies in the Development and Uses of Complex Data Bases," and Part VII, which includes Stanley Rothman, "Protecting Privacy: Pros and Cons;" Edgar L. Feige and Harold W. Watts, "Protection of Privacy through Micro-aggregation;" and Joseph Steinberg, "Some Aspects of Statistical Data Linkage for Individuals."

Boruch, Robert F. "Assuring Confidentiality of Responses in Social Research: A Note on Strategies." *The American Sociologist*, 6:4 (November 1971), 308-311.

Two strategies are proposed to obtain a truthful response without jeopardy to respondent or questioner: (1) The Greenberg randomized-response technique, requiring extensive statistical manipulation; and (2) a technique based on administrative models needing only logistical, mechanical manipulation. Each technique is explained and then analyzed in terms of associated methodological difficulties.

_____. "Educational Research and the Confidentiality of Data: A Case Study." *Sociology of Education*, 44:1 (Winter 1971), 59-85.

Examines the privacy issue with respect to the information system which comprises the basis for the American Council on Education Higher Education Data Bank. A brief overview of the relevant literature is provided.

_____. "Maintaining Confidentiality of Data in Educational Research: A Systemic Analysis." *American Psychologist*, 26:5 (May 1971), 413-430.

An extensively referenced overview of existing methods of assuring confidentiality of data in longitudinal research systems using statistical data banks. A variety of methods are analyzed with respect to their effectiveness in promoting the anonymity of respondents and, secondarily, the security of the data itself.

_____. "Relations Among Statistical Methods for Assuring Confidentiality of Social Research Data." *Social Science Research*, 1:4 (December 1972), 493-414.

Three randomized response methods—the Warner Technique, the Greenberg unrelated question model, and the Boruch contamination model are compared. Also discussed are the legal protection advantages afforded the data by the use of such methods.

_____. "Strategies for Eliciting and Merging Social Research Data." *Policy Sciences*, 3:3 (September 1972), 275-295.

Study of means of merging records from separate files while prohibiting the identification of individuals in at least one of the files. Three general models of data banks are discussed: "insulated data banks," "brokerage models," and "code linkage systems."

Breckenridge, Adam Carlyle. *The Right to Privacy*. Lincoln, Nebraska: University of Nebraska Press, 1970.

Discussion of cases in Great Britain and the United States involving arbitrary and unreasonable intrusions on privacy.

British Computer Society. *Privacy and the Computer—Steps to Practicality*, edited by L. Ellis. London: The British Computer Society, 1972.

Canada. Department of Communications, and Department of Justice. *Privacy and Computers*. Ottawa: Information Canada, 1972.

Report of a Task Force on Privacy and Computers established by the Departments of Communication and Justice in 1971. Includes a study of the value of privacy, a summary of empirical studies of the present state of information processing in Canada in both the public and private sectors, and an analysis of the legal system and the protection of privacy.

_____. *Statistical Data Banks and Their Effects on Privacy*. A study for the Privacy and Computers Task Force by H.S. Gellman. Ottawa: Information Canada, 1972.

_____. Parliament. *An Act to Provide for Data Surveillance and Privacy*. Bill 46, 28th Legislature, 3rd sess., 19 Eliz. 2, 1970.

Canadian Institute of Chartered Accountants. Study Group on Computer Control and Audit Guidelines. *Computer Control Guidelines*. Toronto: The Canadian Institute of Chartered Accountants, 1970.

Cantril, Albert H., and Charles W. Roll, Jr. *Hopes and Fears of the American People*. A Potomac Associates Book. New York: Universe Books, 1971.

A report of two public opinion surveys in 1971 of public views on a number of political issues.

Caro, Francis G., ed. *Readings in Evaluation Research*. New York: Russell Sage Foundation, 1971.

Clark, John O. E. *Computers at Work*. A Bantam Book. New York: Grosset & Dunlap, Inc., 1973.

Describes applications of computers that affect people and their work.

Columbia Human Rights Law Review, 4:1 (Winter 1972).

The entire issue is devoted to the debate on privacy. Articles include:

- Arthur R. Miller, "Computers, Data Banks and Individual Privacy: An Overview."
 Sam J. Ervin, Jr., "The First Amendment: A Living Thought in the Computer Age."
 Nicholas deB. Katzenbach and Richard W. Tomc, "Crime Data Centers: The Use of Computers in Crime Detection and Prevention."
 Frank Askin, "Surveillance: The Social Science Perspective."
 Michael A. Baker, "Record Privacy as a Marginal Problem: The Limits of Consciousness and Concern."
 John P. Flannery, "Commercial Information Brokers."

"Comments: Evidence- Privileged Communication - Extension of the Privilege to Communication Involving Agents." *Michigan Law Review*, 50:2 (December 1951), 308-315.

Committee on Information in the Behavioral Sciences. *Communication Systems and Resources in the Behavioral Sciences*. Washington, D.C.: National Academy of Sciences, 1967.

Computer and Business Equipment Manufacturers Association. *The Role of Computers in Privacy, Confidentiality, Data Security*. Washington, D.C.: Computer and Business Equipment Manufacturers Association, 1973. (Pamphlet.)

"Computers: To Dedicate or Not To Dedicate, That is the Question." *The Bureaucrat*, 1:4 (Winter 1972), entire issue.

A collection of articles on the issue of integrated versus dedicated computer systems.

Conference Board of the Mathematical Sciences. Committee on Computer Education. *Recommendations Regarding Computers in High School Education*. Washington, D.C.: Conference Board of the Mathematical Sciences, 1972.

Conrad, Herbert S. "Clearance of Questionnaires With Respect to 'Invasion of Privacy, Public Sensitivities, Ethical Standards, Etc.'" *American Psychologist*, 22:5 (May 1967), 356-359.

Cortés, Irene R. *The Constitutional Foundations of Privacy*. Quezon City, Philippines: University of the Philippines Law Center, 1970.

A discussion of the nature of privacy and the development of the concept of privacy as a tort and in constitutional law in the United States, Great Britain, and the Philippines.

Council of Social Science Data Archives. *Social Science Data Archives in the United States, 1967*. New York: Council of Social Science Data Archives, 1967.

Brief description of the contents, availability of data, equipment, and publications of 25 social data archives.

Countryman, Vern. "The Diminishing Right of Privacy: The Personal Dossier and the Computer." *Texas Law Review*, 49:5 (May 1971), 8-21, 27.

Lists dossier-compiling activities of the FBI, IRS, Census Bureau, House Internal Security Committee, Armed Services, credit bureaus, investigative reporting agencies, and "punitive compilers." The paper argues that the proliferation of computerized dossiers must be curtailed since legislation will not adequately restrict use of personal dossiers or protect personal privacy.

Curran, William J.; Barbara Stearns; and Honora Kaplan. "Privacy, Confidentiality and Other Legal Considerations in the Establishment of a Centralized Health-Data System." *New England Journal of Medicine*, 281: 5 (July 31, 1969), 241-248.

On the legal issues raised in establishing a health data system. Codes of ethics, criminal and civil penalties, interagency agreements, and a system of public surveillance to protect individual privacy and the confidentiality of data are discussed.

Daechsel, Werner F. O. "Problems Arising from Universal Numbering and Record Linkage Systems." *Canadian Hospital*, 49:3 (March 1972), 23-24.

Data Processing Management Association. "Codes of Conduct and Good Practice for CDP Holders To Be Developed by Certification Council." News Release. Chicago, May 1972.

Ditchley Foundation. *Private Rights and Freedom of the Individual*. Ditchley Paper No. 41. Ditchley Park, Ernstone, Oxfordshire, England: The Ditchley Foundation, 1972.

Report of a conference, April 7-10, 1972, at Ditchley Park to study government need for social data, government intrusions into private life, and safeguards to prevent unjustified intervention.

DuBois, N. S. D'Andrea. "On the Problem of Matching Documents with Missing and Inaccurately Recorded Items." *Annals of Mathematical Statistics*, 35 (September 1964), 1404-1405.

Elias, Stephan R., and Trudy Rucker. "Knowledge is Power: Poverty Law and the Freedom of Information Act." *Clearinghouse Review*, VI:1 (May 1972), 1-15.

Discussion of exemptions 2, 3, 4, 5, and 7 of the Freedom of Information Act and their implications for the release of records of use to poverty lawyers.

Ernst, Martin L. *Management, the Computer and Society*. Cambridge, Mass.: Arthur D. Little, Inc., n.d. (Pamphlet.)

Ernst, Morris L., and Alan U. Schwartz. *Privacy: The Right to Be Let Alone*. Milestones of Law Series. New York and London: The Macmillan Co., 1962.

Written for the layman. Describes major cases in the development of law on privacy.

Federal Republic of Germany. Hesse State Parliament. Data Protection Commissioner. *First Activity Report*. Document 7/1495. 1972.

Evaluates the weakness of the Hesse Data Protection Act. It describes the development of data processing and the legal regulation of access to personal information in administrative records in the various German states, at the federal level, and in the United States, the United Kingdom, and France. Recommendations for specific safeguards are offered.

Hessischer Landtag. Datenschutzbeauftragter. Zweiter Tätigkeitsbericht. Drucksache 7/3137. 1973. [Hesse State Parliament. Data Protection Commissioner. Second Activity Report. Document 7/3137. 1973 (in German).]

Feige, Edgar L., and Harold W. Watts. "An Investigation of the Consequences of Partial Aggregation of Micro-economic Data." *Econometrica*, 40:2 (March 1972), 363-360.

Feldzamen, A. N. *The Intelligent Man's Easy Guide to Computers*. New York: David McKay Company, Inc., 1971.

Fellegi, I. P. "On the Question of Statistical Confidentiality." *Journal of the American Statistical Association*, 67:337 (March 1972), 7-18.

———, and Alan B. Sunter. "A Theory for Record Linkage." *Journal of the American Statistical Association*, 64:328 (December 1969), 1183-1210.

Fishman, Phillip F. "Expungement of Arrest Records: Legislation and Litigation to Prevent Their Abuse." *The Clearinghouse Review*, VI:12 (April 1973), 725-733.

Forsyth, Frederick. *The Day of the Jackal*. New York: The Viking Press, 1971.

A fictional account of an attempt to assassinate the late French President Charles de Gaulle. The potential assassin acquires a series of false identities by manipulating the official recordkeeping systems of several countries. However, he has no identity of his own since he himself is not listed in a record-keeping system.

France. Conseil d'Etat. *Rapport annuel 1969-1970. Troisième partie: Réformes d'ordre législatif, réglementaire ou administratif. Deuxième étude: Les conséquences du développement de l'informatique sur les libertés publiques et privées et sur les décisions administratives*. (Unpublished.)

Fried, Charles. "Privacy." *The Yale Law Journal*, 77:3 (January, 1968), 475-93.

"Functional Overlap between the Lawyer and Other Professionals: Its Implications for the Privileged Communications Doctrine." *Yale Law Review*, 71:7 (June 1962), 1226-1273.

Gallatin, Judith, and Joseph Adelson. "Legal Guarantees of Individual Freedom: A Cross-National Study of the Development of Political Thought," *Journal of Social Issues*, 27:2 (1971), 93-108.

Paper presents the findings of a study comparing attitudes of British, German, and American adolescents towards two proposed laws that could involve an invasion of privacy.

Gibson, R. Dale, and John M. Sharp. "Privacy and Commercial Reporting Agencies." Legal Research Institute, University of Manitoba, Winnipeg, October 1968.

Gilchrist, Bruce, and Milton R. Wessel. *Government Regulation of the Computer Industry*. Montvale, N. J.: AFIPS Press, 1972.

Goldberg, Edward M. "Privacy Problems in Municipal Information Systems." Prepared under the auspices of Municipal Systems Research, Claremont Graduate School, U.S. Department of Housing and Urban Development Contract H-1594, May 1972.

Great Britain. Civil Service Department. *Computers in Central Government Ten Years Ahead*. Civil Service Department Management Studies 2. London: H. M. Stationery Office, 1971.

———. Home Office. *Report of the Committee on Privacy*, Rt. Hon. Kenneth Younger, chairman. London: H. M. Stationery Office, 1972.

The Final Report of a committee established in 1970 to review the need for legislation to protect "individuals and commercial and industrial interests" from invasion of privacy. The report examines the nature of privacy, complaints of invasion of privacy, the adequacy of present law in protecting against invasion of privacy, the disclosure of confidential information, and the creation of a general right of privacy.

———. *Report of the Departmental Committee on Section 2 of the Official Secrets Act 1911*. Lord Franks, chairman. H. M. Stationery Office, 1972.

Vol. 1 Report of the Committee

Vol. 2 Written Evidence Submitted to the Committee

Vol. 3 Oral Evidence

Vol. 4 Oral Evidence. Mainly from non-Government Witnesses.

Review and recommendations for change in the operation of the Official Secrets Act 1911.

- _____. House of Commons Library Research Division. *Reference Sheet; Privacy*. Ref. 69/7. 4 March 1969.
- A list of newspaper and periodical articles, publications of the National Council for Civil Liberties, parliamentary material, and law relating to privacy.
- Greenberg, Bernard S., et al. "The Unrelated Question Randomized Response Model: Theoretical Framework." *Journal of the American Statistical Association*, 64:326 (June 1969), 520-539.
- Greenberger, Martin, ed. *Computers, Communications, and the Public Interest*. Baltimore and London: Johns Hopkins Press, 1971.
- A collection of papers that examine the problem of preserving traditional human rights and values in view of man's increasing reliance on computer technology. See especially Chapter V, "Civil Liberties and Computerized Data Systems, and Chapter VII, "Developing National Policy for Computers and Communications.
- Gregory, Charles O., and Harry Kalven. *Cases and Materials on Torts*. Boston: Little, Brown and Company, 1969.
- See especially Chapter 16, "A Preface to the Study of Unfair Commercial Practices as Torts."
- Grenier, Edward J., Jr. "Computers and Privacy: A Proposal for Self-Regulation." *Duke Law Journal*, 1970:3 (June 1970), 495-513.
- Gross, Hyman. "The Concept of Privacy." *New York University Law Review*, 42:8 (March 1967), 34-54.
- Grunfeld, Y., and Z. Griliches. "Is Aggregation Necessarily Bad?" *The Review of Economics and Statistics*, 42:1 (February 1970), 1-13.
- Hamilton, Peter. *Computer Security*. London: Cassell/Associated Business Programmes Ltd., 1972.
- Examines vulnerabilities arising from the society's increasing dependence on computers and suggests means by which these vulnerabilities may be reduced.
- _____. *Espionage and Subversion in an Industrial Society*. London: Hutchinson & Co. Ltd., 1967.
- On the extent of industrial espionage, its dangers, and means of protecting against it.
- Hansen, Morris H. "Insuring Confidentiality of Individual Records in Data Storage and Retrieval for Statistical Purposes." *American Federation of Information Processing Societies Proceedings: Fall Joint Computer Conference*, 39 (Fall 1971), 579-585.

- Harrison, Annette. *The Problem of Privacy in the Computer Age: An Annotated Bibliography*. 2 Vols. Santa Monica, Calif.: The Rand Corporation, 1967.
- Hartnett, Rodney T., and Harriet C. Seligson. "The Effects of Varying Degrees of Anonymity on Responses to Different Types of Psychological Questionnaires." *Journal of Educational Measurement*, 4:2 (Summer 1967), 95-103.
- Hendrickson, Robert. *The Cashless Society*. New York: Dodd, Mead & Co., 1972.
- A discussion of the increasing reliance on credit systems and its implications for individual freedom.
- Hilmar, Norman A. "Anonymity, Confidentiality, and Invasions of Privacy: Responsibility of the Researcher." *American Journal of Public Health*, 58:2 (February 1968), 324-330.
- Hoffman, Lance J. "The Formulary Model for Flexible Privacy and Access Controls." *American Federation of Information Processing Societies Proceedings: Fall Joint Computer Conference*, 39 (Fall 1971), 587-601.
- _____, and W. F. Miller. "Getting a Personal Dossier from a Statistical Data Bank." *Datamation*, 16:5 (May 1970), 74-75.
- Hoglund, John A., and Jonathan Kahan. "Invasion of Privacy and the Freedom of Information Act. Getman v. NLRB." *George Washington Law Review*, 40:3 (March 1972), 527-541.
- An examination of some implications of the Freedom of Information Act and its exemption 6, allowing agencies to withhold files containing personal data if releasing the information would constitute a "clearly unwarranted invasion of personal privacy."
- Hoos, Ida R. *Systems Analysis in Public Policy: A Critique*. Berkeley, Calif.: University of California Press, 1972.
- Institute for Defense Analyses. *Task Force Report: Science and Technology*. A Report to The President's Commission on Law Enforcement and Administration of Justice. Washington, D.C.: U.S. Government Printing Office, 1967.
- "Integrated Municipal Information Systems." *Nation's Cities*. January 1972, 10-39.
- A summary of *Integrated Municipal Information Systems: The USAC Approach*.
- International Commission of Jurists. "The Protection of Privacy." *International Social Science Journal*, 24:3 (1972).

A comparative survey of the legal protection of privacy in ten countries: Argentina, Brazil, Federal Republic of Germany, France, Mexico, Sweden, Switzerland, the United Kingdom, the United States, and Venezuela. Includes Paul J. Miller and H. H. Kuhlmann, "Integrated Information Bank Systems, Social Book-Keeping and Privacy," as well as essays treating the implications for privacy of technological developments, and general law on privacy, invasion of privacy, and disclosure of private information.

Jones, R. V. "Some Threats of Technology to Privacy." *Proceedings of the 3rd International Colloquy about the European Convention of Human Rights*. Brussels, 1970.

Junior Chamber International. *Misuse of Computer Information*. Coral Gables, Florida: Junior Chamber International, 1972. (Pamphlet.)

Justice. (British Section of the International Commission of Jurists.) *Privacy and the Law*. Mark Littman and Peter Carter-Ruck, chairmen. London: Stevens & Sons Limited, 1970.

Summarizes present law relating to privacy in England, France, Germany, and the United States. Appendix A includes a bibliography of literature on law and privacy in the United Kingdom, Canada, France, Germany, Japan, Sweden, Switzerland, and the United States. Appendix B—"Conclusions of the Nordic Conference on the Right of Privacy. Appendix J—"Draft Right of Privacy Bill." Appendix K—"Summary of Recommendations Made by the Joint Working Party of Justice and the British Committee of the International Press Institute in their Report, 'The Law and the Press,' 1965."

Katz, Jay. *Experimentation With Human Beings: The Authority of the Investigator, Subject, Profession, and State in the Human Experimentation Process*. New York: Russell Sage Foundation, 1972.

Kennedy, J. M. *Linkage of Birth and Marriage Records Using a Digital Computer*. Chalk River, Ontario: Atomic Energy of Canada Limited, 1961.

Kent State University. Center for Urban Regionalism. *Urban and Regional Information Systems: Past, Present, and Future*. Papers from the 8th Annual Conference of the Urban and Regional Information Systems Association, Louisville, Kentucky, September 3-5, 1970.

Kershaw, David N., and Joseph C. Small. "Data Confidentiality and Privacy: Lessons from the New Jersey Negative Income Tax Experiment." *Public Policy*, 20:2 (Spring 1972), 257-280.

Kiefer, Charles, and James L. Lewis. *Federal-State-Local Cooperative Systems*. Prepared for U.S. Department of Health, Education, and Welfare, Health Services and Mental Health Administration. Washington, D.C.: Moshman Associates, 1972.

Krauss, Leonard I. *Computer-Based Management Information Systems*. New York: American Management Association, Inc., 1970.

Kruskal, William. "The Committee on National Statistics." *Science*, 180:4092 (22 June 1973), 1256-1258.

Lawyers' Committee for Civil Rights Under Law. *Law and Disorder III: State and Federal Performance Under Title I of the Omnibus Crime Control and Safe Streets Act of 1968*. Washington, D.C.: Lawyers' Committee for Civil Rights Under Law, 1973.

Lenk, Klaus. *Automated Information in Public Administration—Present Developments and Impact*. Paris: Organisation for Economic Co-operation and Development, 1972.

Liethen, Michael A. "Release of Student Records at the University of Wisconsin and the Wisconsin Public Records Statute." University of Wisconsin School of Law, June 1972.

Loth, David, and Morris L. Ernst. *The Taming of Technology*. New York: Simon and Schuster, 1972.

Describes legal means of controlling potentially harmful aspects of technological growth. See Chapter 17, "Law and the Computer," for a list of significant court cases involving invasion of privacy. Proposals for the regulation of data banks are offered.

Lundsgaarde, Henry P. "Privacy: An Anthropological Perspective on the Right to Be Let Alone." *Houston Law Review*, 8 (1970-71), 858-875.

Lusky, Louis. "Invasion of Privacy: A Clarification of Concepts." *Political Science Quarterly*, LXXXVII:2 (June 1972), 192-209.

Criticizes a unitary definition of privacy. Argues that the formulation of legislation protecting privacy must be preceded by a consideration of the existence of two types of information transfer: the transfer of personal information against the will of the individual, and the transfer of false or misleading information about an individual.

McKinley, Charles, and Robert W. Frase. *Launching Social Security: A Capture-and-Record Account: 1935-1937*. Madison: The University of Wisconsin Press, 1970.

Massachusetts Institute of Technology. *Final Report of the Ad Hoc Committee on the Privacy of Information at MIT*. Cambridge, Mass.: Massachusetts Institute of Technology, 1971.

Medical Information Bureau. *A History of the Automated M.I.B. System*. New York: Medical Information Bureau, n.d.

Pamphlet on the development and future uses of the Medical Information Bureau.

_____. *The Automated M.I.B.* New York: Medical Information Bureau, revised November 1971.

A brief description of the Medical Information Bureau's service to life insurance companies.

Metzner, Charles A. "Data Banks: Fundamental Considerations." *American Journal of Public Health*, 60:10 (October 1970), 1984-1990.

A paper presented before a Joint Session of the Statistics and Medical Care Sections of the American Public Health Association, November 11, 1969.

From the Introduction:

"A consideration of the potential and limitation of data banks. . . Data banks should be considered not simply in technical terms, but of at least equal significance with respect to social, political, and ethical issues."

Miller, Arthur R. *The Assault on Privacy: Computers, Data Banks, and Dossiers*. Ann Arbor: University of Michigan Press, 1971; and a Signet Book. New York: The New American Library, 1972.

A much cited work on technological threats to personal privacy.

Miller, Herbert S. *The Closed Door: The Effect of a Criminal Record on Employment with State and Local Public Agencies*. Washington, D.C.: Georgetown University Law Center, Institute of Criminal Law and Procedure, 1972.

Moss, Judith, "Confidentiality and Identity." *Socio-Economic Planning Sciences*, 4:1 (March 1970), 17-25.

Nagi, Saad L. *Disability and Rehabilitation*. Columbus, O.: Ohio State University Press, 1969.

National Academy of Sciences - National Research Council. Division of Medical Sciences. Drug Research Board. *Report of the International Conference on Adverse Reactions Reporting Systems, October 22-23, 1970*. Washington, D.C.: National Academy of Sciences, 1971.

See proposal for a National Center for Drug Surveillance.

National Accreditation Council for Agencies Serving the Blind and Visually Handicapped. "Confidentiality and the School: A New Outlook Symposium." *The New Outlook for the Blind*, 67:2 (February 1973), 49-65.

_____. "Standards for Confidentiality." New York, April 1972.

National Association for State Information Systems and the State of Illinois. *1970 NASIS Report. Information Systems Technology in State Government*. Available from the Council of State Governments, Lexington, Kentucky.

Summary of the first annual NASIS survey on current use and future trends of statewide computerized information systems.

_____ in conjunction with the States. *1971 NASIS Report. Information Systems Technology in State Government*. Available from the Council of State Governments, Lexington, Kentucky.

Summary of the second annual NASIS survey on current use and future trends of statewide computerized information systems.

National Council on Crime and Delinquency. "Bay Area Counties Probation Research Project: Proposed Security and Privacy Procedures for Information Collected." Hackensack, New Jersey, n.d.

_____. "Security and Privacy in the Parole Decision-Making Project," Hackensack, New Jersey, n.d.

_____. "Security and Privacy in the Uniform Parole Reports Program." Hackensack, New Jersey, n.d.

National League for Nursing, Inc. "Policy and Procedures Regarding Research Investigations Involving Human Subjects." New York, revised March 1969.

National Social Welfare Assembly, Inc. Ad hoc Committee on Confidentiality. *Confidentiality in Social Services to Individuals*. New York: National Social Welfare Assembly, 1958.

Nejelski, Paul, and Lindsey M. Lerman. "A Researcher-Subject Testimonial Privilege: What to Do before the Subpoena Arrives." *Wisconsin Law Review*, 4:1 (Fall 1971), 1085-1148.

Newcombe, H. B., and J. M. Kennedy. "Record Linkage: Making Maximum Use of the Discriminating Power of Identifying Information." *Communications of the Association for Computing Machinery*, 5:11 (November 1962), 563-566.

Niblett, G.B.F. *Digital Information and the Privacy Problem*. OECD Informatics Studies, No. 2. Paris: Organisation for Economic Co-operation and Development, 1971.

An examination of current problems of data confidentiality and computerized information systems in OECD nations. Discusses professional standards,

technological safeguards, administrative practices, legal remedies and sanctions, and new legislation. See Appendix I for a summary of OECD nation replies to a questionnaire on privacy.

Noble, John N., Jr. "Protecting the Public's Privacy in Computerized Health and Welfare Systems." *Social Work*, 16:1 (January 1971), 35-41.

Discusses privacy and confidentiality issues raised by computerized health and welfare systems, and suggests guidelines for the development of such systems. A revision of a paper presented at the Massachusetts Conference on Social Welfare, Boston, December 3, 1969.

———, and Henry Wechsler. "Obstacles to Establishing Communitywide Information Systems on Health and Welfare." *Welfare in Review*, 8:6 (November-December 1970), 18-26.

Report of a 15-month study of record-keeping practices of 183 health and social service organizations. Addresses the practical difficulties likely to be encountered in developing an automated national reporting system of health and social conditions.

Northwest Regional Educational Laboratory. Relevant Educational Applications of Computer Technology. *Course I: Computers in Education: A Survey. Book 5: The Social Impact of Computers*. San Carlos, Calif.: Technica Education Corporation, 1971.

Vol. 5 of a 24-volume training course on computers and education. Developed primarily for school administrators and teachers. All textbooks are to be used in conjunction with a computer. Programs in Vol. 5 were designed to demonstrate moral, social, educational, and political implications of the computer for society.

Oettinger, Anthony G. *Run, Computer, Run*. Harvard Studies in Technology and Society. Cambridge, Mass.: Harvard University Press, 1969.

Olafson, Freya; Allen Ferguson, Jr.; and Alberta W. Parker. *Confidentiality: A Guide for Neighborhood Health Centers*. Neighborhood Health Center Seminar Program Monograph Series No. 1. San Francisco: Pisani Printing Co., 1971.

A study of legal and ethical aspects of confidentiality of patient information and records maintained by neighborhood health centers. Applicable state laws in California, Alabama, New York, and Ohio are included.

Organisation for Economic Co-operation and Development. Directorate for Scientific Affairs. Computer Utilisation Group. *Inventory of Data Banks in the Public Sector*. OECD Informatics Studies. Paris: Organisation for Economic Co-operation and Development, 1971.

Packard, Vance. *The Naked Society*. New York: David McKay Company, Inc., 1964.

An exposé of government and big business snooping into the private lives of citizens.

Parker, Donn B. "The Rules of Ethics in Information Processing." *Communications of the American Council on Education*, 11:3 (March 1968), 198-201.

Pastalan, Leon A. "Privacy as a Behavioral Concept." *Social Science*, 45:2 (April 1972), 93-17.

"The purpose of this paper is to propose an operational definition of privacy; to suggest a typology of modes of privacy; and to derive potential research payoffs through the use of a matrix model linking the various modes of privacy to a series of related situational contingencies." (from the paper)

Peck, Paul L. *Survey of Applicable Safeguards for Insuring the Integrity of Information in Data Processing Environment*. McLean, Va.: The MITRE Corporation, 1971.

Pipe, Russell. *Data Base Developments and International Dimensions*. Paris: Organisation for Economic Co-operation and Development, 1972.

"Privacy." *Law and Contemporary Problems*, 31:2 (Spring 1966), entire issue.

From the Table of Contents:

William M. Beaney, "The Right to Privacy and American Law;"

Milton R. Konvitz, "Privacy and the Law: A Philosophical Prelude;"

Edward Shils, "Privacy: Its Constitution and Vicissitudes;"

Sidney M. Jourard, "Some Psychological Aspects of Privacy;"

Harry Kalven, Jr., "Privacy in Tort Law—Were Warren and Brandeis Wrong?";

Kenneth L. Karst, " 'The Files': Legal Controls Over the Accuracy and Accessibility of Stored Personal Data;"

Joel F. Handler and Margeret K. Rosenheim, "Privacy in Welfare: Public Assistance and Juvenile Justice;" and

William A. Creech, "The Privacy of Government Employees."

"Privacy and Efficient Government: Proposals for a National Data Center." *Harvard Law Review*, 82:2 (December 1968) 400-417.

Project SEARCH. Committee on Security and Privacy. *Security and Privacy Considerations in Criminal History Information Systems*. Technical Report No. 2. Sacramento, Calif.: Project SEARCH Staff. California Crime Technological Research Foundation, 1970.

A guide to privacy and security considerations for systems involving interstate exchange of criminal histories. Includes discussion of privacy problems likely to be encountered in such systems, proposed privacy policy, safeguards, and codes of ethics, and security arrangements used by Project SEARCH staff.

_____, and U.S. Department of Justice, Law Enforcement Assistance Administration. *Symposium on Criminal Justice Information and Statistics Systems*. New Orleans, October 3-5, 1972.

From the Table of Contents:

Session I	Advancements in Criminal Justice Information and Statistics Systems
Session IIA	Police Information and Statistics
Session IIB	Courts Information and Statistics
Session IIC	Corrections Information and Statistics
Session IID	Criminal Justice Information Systems Design and Implementation
Session IIE	Identification Systems
Session IIF	Information for Criminal Justice Planning
Session III	Major Issues in Criminal Justice Information and Statistics Systems
Session IV	Developing Trends in Information and Statistics

Prosser, William H. "Privacy." *California Law Review*, 48:3 (August 1960), 383-423.

"Protecting the Subjects of Credit Reports." *The Yale Law Journal*, 80:5 (April 1971), 1035-1069.

Pylyshyn, Zenon W., ed. *Perspectives on the Computer Revolution*. Englewood Cliffs, N. J.: Prentice Hall, Inc., 1970.

From the Introduction:

"The book is divided conceptually into three parts. The first is devoted to the development of computers and the intellectual heritage of computer science. The second part emphasizes the relationship between man—as a conscious thinking organism—and machines. The last part bears primarily on the relationship between society as a whole and the machine."

Readings include Edmund C. Berkeley, "Social Responsibility of Computer People," and Alan F. Westin, "Legal Safeguards to Insure Privacy in a Computer Society." The latter article suggests general legal principles and administrative and systems safeguards to protect against "data surveillance."

Rainwater, Lee, and David J. Pittman. "Ethical Problems in Studying a Politically Sensitive and Deviant Community." *Social Problems*, 14:4 (Spring 1967), 357-366.

Reubhausen, Oscar M., and Orville G. Brim, Jr. "Privacy and Behavioral Research." *Columbia Law Review*, 65:7 (November 1965), 1184-1211.

"Right to Privacy: Social Interests and Legal Right." *Minnesota Law Review*, 51:531 (1967), 531-551.

Rosander, A. C. "Analysis of the Kaysen Committee Report." *The American Statistician* 24:1 (February 1970), 20-25.

Rossi, Peter H. and Walter Williams, eds. *Evaluating Social Programs: Theory, Practice, and Politics*. Quantitative Studies in Social Relations. New York and London: Seminar Press, 1972.

Study addresses three questions: Why has so little evaluative research been undertaken? What problems are there in developing evaluative research and using its results? What should government and social scientists do to encourage evaluative research?

Rothman, Stanley, and Charles Mosmann. *Computers and Society*. Chicago: Science Research Associates, Inc., 1972.

Rowe, B. C. ed. *Privacy, Computers and You*, Manchester, England: The National Computing Centre Limited, 1972.

A collection of papers presented at the Workshop on the Data Bank Society, London, November 18-19, 1970, sponsored by the National Council for Civil Liberties and Allen & Unwin Limited. See papers on privacy in a technological society; the use of data banks by physicians, psychologists, banks, and credit bureaus; trade unions and data banks; and proposals for technical, legal, and ethical safeguards of privacy.

Rule, James B. *Private Lives and Public Surveillance*. London: Allen Lane, 1973.

Considers the use of personal information as a means of social control. The record-keeping activities involved in police record systems, vehicle and driver licensing, and National Insurance in Great Britain, and consumer credit and the Bank Americard systems in the United States are analyzed.

Russell Sage Foundation. *Guidelines for the Collection, Maintenance and Dissemination of Pupil Records*. Report of a Conference on the Ethical and Legal Aspects of School Record Keeping, Sterling Forest, N.Y., May 25-28, 1969.

Recommendations for limiting access to personal data in school records.

_____. *Student Records in Higher Education: Recommendations for the Formulation and Implementation of Record-Keeping Policies in Colleges and Universities*. New York: Russell Sage Foundation. Forthcoming.

Ryan, G. A., and K. E. Monroe. *Computer Assisted Medical Practice: The AMA's Role*. Chicago: American Medical Association, 1971.

A guide to the use of computers by physicians. Includes short commentaries on automated patient histories, medical records, confidentiality, ethical concerns, and legal restraints.

Sackman, Harold, and Barry W. Boehm. *Planning Community Information Utilities*. Montvale, N.J.: AFIPS Press, 1972.

_____, and Harold Borko, eds. *Computers and the Problems of Society*. Montvale, N.J.: AFIPS Press, 1972.

_____, and Norman Nie, eds. *The Information Utility and Social Choice*. Montvale, N. J.: AFIPS Press, 1970.

A group of papers prepared for a conference sponsored by the University of Chicago, the Encyclopedia Britannica, and the American Federation of Information Processing Societies. The papers address the desirable uses of mass information utilities and the effects of direct citizen participation upon political processes.

Salancik, Gerald R.; Theodore J. Gordon; and Neale Adams. *On the Nature of Economic Losses Arising from Computer-Based Systems in the Next Fifteen Years*. Menlo Park, Calif.: Institute for the Future, 1972.

Samuelson, Erik. *Statlige databanker og personlighets vern* [Public Data-Banks and the Defense of Privacy]. Oslo: Universitets Forlaget, 1972.

Sawyer, Jack, and Howard Schechter. "Computers, Privacy, and the National Data Center: The Responsibility of Social Scientists." *American Psychologist*, 23:11 (November 1968), 810-818.

Schoenfeldt, Lyle F. "Data Archives as Resources for Research, Instruction, and Policy Planning." *American Psychologist*, 25:7 (July 1970), 609-616.

Shiskin, Julius. "Reorganization of Federal Statistical Activities." *Statistical Reporter*, 72-5 (November 1971), 80-83.

Statement given before the Joint Economic Committee, October 27, 1971. Brief description of proposed statistical reorganization of the Departments of Agriculture, Commerce, Labor, and Health, Education, and Welfare. Centers of data processing and collection, and data analysis would be established within each of the four departments.

Social Science Research Council. *Report of the Committee on the Preservation and Use of Economic Data to the Social Science Research Council*, Richard Ruggles, chairman. New York: Social Science Research Council, 1965.

Stafford, Samuel. "Is the Social Security Number Being Abused?" *Government Executive*, 4:6 (June 1972), 62-63.

Stallings, Wayne. *A Confidentiality and Public Access Policy for Local Government*. Prepared for the Charlotte Integrated Municipal Information System Project. Chapel Hill: University of North Carolina, Department of City and Regional Planning, 1972.

Third in a series of papers prepared for the Charlotte IMIS Project. Examines current use of public records and proposes a classification system to control access to personal information held by local government.

Stanford University. *Report of the Ad Hoc Committee on Protection of Privacy of Information at Stanford*. Stanford, Calif.: Stanford University, 1972.

State of California. Intergovernmental Board on Electronic Data Processing. *Policy Statement on Privacy and Security*. Sacramento, Calif.: State Printing Office, 1971.

_____. Legislature. Assembly. Committee on Statewide Information Policy. *Final Report*. Sacramento, Calif.: State Printing Office, March 1970.

A Study of the implications of computerized information systems for personal privacy. Includes a discussion of the right to privacy in California and the California Public Records Act of 1968. See Appendix B, "Opinion of Legislative Counsel Relating to the Right of Privacy in California;" Appendix C "Opinion of Legislative Counsel Relating to Public Records Involving Individuals;" Appendix E, "Statewide Information Policy Committee Questionnaire and Responses;" Appendix F, "Opinion of Legislative Counsel: A Digest of Laws Relating to Collection, Retention, and Destruction of Records;" and Appendix G, "Opinion of Attorney General Relating to Availability for Public Inspection of Records of the Board of Pilot Commissioners."

State of Illinois. Department of Finance. Management Information Division. *Impact '70s. Illinois Master Plan Applying Computer Technology in the 1970's*. Vol. II: *Detailed Development*. April 23, 1971.

A comprehensive plan for the development of computerized information systems in Illinois State government. See discussions of data bank privacy and security, and the State of Illinois proposed code of ethics for EDP personal.

State of Maryland. Department of Mental Hygiene, and the National Institute of Mental Health. *Maryland Psychiatric Case Register: Description of History, Current Status and Future Uses*. A Cooperative Research Project of the Maryland Department of Mental Hygiene and the National Institute of Mental Health. Washington, D.C.: U.S. Department of Health, Education, and Welfare, December 1967.

Description of the Maryland register of cumulative records of residents receiving treatment from a psychiatric hospital in Maryland or the District of Columbia since July 1, 1969. Includes comment on current and future uses of the information and on confidentiality of data in the register.

State of New York. Insurance Department. *Report on Examination of the Medical Information Bureau*, by Harvey N. Ginsberg. March 15, 1967.

Brief report on the history, purpose, and operation of the Medical Information Bureau. Includes an outline of procedures for handling complaints of individuals and insurance companies.

_____. Supreme Court. First and Second Judicial Departments. Appellate Divisions. The Departmental Committees for Court Administration. *Automation in the Courts: Its Impact on Record-Making and Record-Keeping; Implications for the Private Citizen and the Public. Symposium, New York, November 1971.*

Steinberg, Joseph, and Hayman C. Cooper. "Social Security Statistical Data, Social Science Research, and Confidentiality." *Social Security Bulletin*, 30:10 (October 1967), 3-15.

_____, and Leon Pritzker. "Some Experiences With and Reflections on Data Linkage in the United States." Paper presented at the 36th Session of the International Statistical Institute, Sydney, Australia, 1967.

Stephens, Jerome. "Biomedical Research and the Need for a Public Policy." Paper prepared for the annual meeting of the American Political Science Association, Washington, D.C., September 5-9, 1972.

Paper on the inadequate protection of persons who are subjects of biomedical research, including a discussion of the use of disadvantaged Americans as research subjects. Includes comment on current legal remedies, the lack of standardized codes of ethics, and suggestions for the development of future policy.

Sterling, Theodore D. "Access to Data." Letters. *Science*, 173:3998 (20 August 1971), 676-77.

Comment on the inaccessibility of raw research data for public review—in this case, the unavailability of E. Cuyler Hammond's data on smoking. For additional comment, see Ellis Blade. "The Public Aspect of Science." Letters. *Science*, 175:4018 (14 January 1972), 123; and Theodore D. Sterling. "Scientific Data: Public or Private?" Letters. *Science*, 175:4018 (14 January 1972), 651.

Stevens, Jean. *Access to Personal Data Files: I*. Freedom of Information Center Report No. 288. Columbia, Missouri: University of Missouri School of Journalism, August 1972.

_____. *Access to Personal Data Files: II*. Freedom of Information Center Report No. 291. Columbia, Missouri: University of Missouri School of Journalism, October 1972.

Stromholm, Stig. *Right of Privacy and Rights of the Personality: A Comparative Survey*. Working paper prepared for the Nordic Conference on Privacy organized by the International Commission of Jurists, Stockholm, May 1967. Stockholm: P.A. Norstedt & Soners Förlag, 1967.

The study is directed to the question of "how to define and protect a person's legitimate interest in being . . . let alone." Examines the nature of privacy and legal rules, legislative initiatives, and standards of private organizations for protecting privacy.

Suchman, Edward A. *Evaluation Research: Principles and Practice in Public Service and Social Action Programs*. New York: Russell Sage Foundation, 1967.

A study of the conception, methodology, and administration of evaluative research on social action programs.

Sweden. Justitiedepartementet. *Data och integritet* [Data and Privacy]. Stockholm: Almqvist & Wikströms Förlaget, 1972.

"Symposium: Computers, Data Banks, and Individual Privacy." *Minnesota Law Review*, 53:2 (December 1968), 211-245.

Lectures from a symposium sponsored by The Merrill Cohen Memorial Fund and the Graduate School of Business Administration, University of Minnesota. Includes Richard Ruggles, "On the Needs and Values of Data Banks;" John de J. Pemberton, Jr., "On the Dangers, Legal Aspects, and Remedies;" Arthur R. Miller, "On Proposals and Requirements for Solutions."

"Symposium on Privacy and the Law." *University of Illinois Law Forum*, 1971:2, 137-178.

Three papers presented at the University of Illinois College of Law, May 7, 1971: Sam J. Ervin, Jr., "Privacy and Government Investigations," on constitutional limitations to government investigation of private citizens; Arthur R. Miller, "The Dossier Society;" and Michael Harrington, "Privacy and the Poor," on the physical lack of privacy experienced by the poor as well as loss of privacy from some welfare requirements. A National Bureaucratic Relations Act is suggested to establish a review board to handle citizen complaints about bureaucracy.

Taviss, Irene, ed. *The Computer Impact*. Englewood Cliffs, N. J.: Prentice-Hall, Inc., 1970.

A collection of papers that consider issues raised by the application of computer technology to the political decision-making process and the economy. See especially, Carl Kaysen, "Data Banks and Dossiers," for a discussion of the need for a national data center and Donald N. Michael, "Speculations on the Relation of the Computer to Individual Freedom and the Right to Privacy," which examines the prospects for freedom and privacy during the next few decades.

"The Computerization of Government Files: What Impact on the Individual?" *UCLA Law Review*, 15:5 (September 1968), 1374-1498.

A discussion of the experiences of the California and Federal governments in computerizing files and the dangers associated with government use of computerized filing systems. Safeguards to prevent unauthorized disclosure of personal information or disclosure of false or misleading information are suggested.

The Conference Board. *Information Technology*, by George Kozmetsky and Timothy Ruefli. Conference Board Report No. 557. New York: The Conference Board, 1972.

Thomas, Uwe. *Computerized Data Banks in Public Administration*. OECD Informatics Studies, No. 1. Paris: Organisation for Economic Co-operation and Development, 1971.

Tillery, Dale. "Seeking a Balance Between the Right of Privacy and the Advancement of Social Research," in *Invasion of Privacy in Research and Testing*, ed. by Warren W. Willingham. *Journal of Educational Measurement Supplement*, 4:1 (Spring 1967), 11-16.

Turn, Rein. *A Brief History of Computer Privacy/Security Research at Rand*. Santa Monica, Calif.: The Rand Corporation, March 1972.

Paper includes a bibliography of Rand publications on data privacy and security.

United Nations. Division of Human Rights. *Seminar on Human Rights and Scientific and Technological Development*. Vienna, Austria, 19 June - 1 July 1972. New York: United Nations, 1972.

_____. Economic and Social Council. Commission on Human Rights. *Human Rights and Scientific and Technological Developments. Report of the Secretary-General. Addendum*. 29 December 1970.

United Presbyterian Church in the U.S.A. "Report of the Task Force on Privacy." Action of the General Assembly. United Presbyterian Church in the U.S.A. 1973 meeting in Omaha, Nebraska, May 15-23, 1973.

U.S. Bureau of the Budget. Office of Statistical Standards. *Review of a Proposal for a National Data Center*, by Edgar S. Dunn, Jr. Statistical Evaluation Report No. 6. Washington, D.C.: U.S. Bureau of the Budget, 1966. Reprinted in U.S. Congress. House. Committee on Government Operations. *The Computer and Invasion of Privacy. Hearings* before a subcommittee of the Committee on Government Operations, House of Representatives, 89th Cong., 2d sess., 1966.

_____. *Report of the Task Force on the Storage of and Access to Government Statistics*. Carl Kaysen, chairman. Washington, D.C.: U.S. Bureau of the Budget, 1966.

U.S. Bureau of the Census. Decennial Census Review Committee. *The Decennial Census: Report to the Secretary of Commerce*. Washington, D.C.: U.S. Government Printing Office, 1971.

U.S. Congress. House. *Confidentiality of Census Information*. Report 91-407, 91st Cong., 1st sess., 1969.

_____. *Fair Credit Reporting. Hearings* before the Subcommittee on Consumer Affairs of the Committee on Banking and Currency, House of Representatives, 91st Cong., 1st sess., 1970.

_____. *1970 Census and Legislation Related Thereto. Hearings* before the Subcommittee on Census and Statistics of the Committee on Post Office and Civil Service, House of Representatives, 91st Cong., 1st sess., 1969. 2 Parts.

_____. *Records Maintained by Government Agencies. Hearings* before a Subcommittee of the Committee on Government Operations, House of Representatives, on H.R. 9527, 92d Cong., 2d sess., 1972.

_____. *Sale or Distribution of Mailing Lists by Federal Agencies. Hearings* before a subcommittee of the Committee on Government Operations, House of Representatives, on H.R. 8903 and Related Bills, 92d Cong., 2d sess., 1972.

_____. *Security and Privacy Criminal Arrest Records. Hearings* before Subcommittee No. 4 of the Committee on the Judiciary, House of Representatives, on H.R. 13315, 92d Cong., 2d sess., 1972.

_____. *The Computer and Invasion of Privacy. Hearings* before a subcommittee of the Committee on Government Operations, House of Representatives, 89th Cong., 2d sess., 1966.

_____. Committee on Science and Astronautics. *The Management of Information and Knowledge*. A compilation of papers prepared for the 11th meeting of the Panel on Science and Technology. Washington, D.C.: U.S. Government Printing Office, 1970.

A collection of papers that analyze the impact of the computer upon society. For a discussion of individual privacy, see Stanford Beer, "Managing Modern Complexity;" Paul Armer, "The Individual: His Privacy, Self-Image, and Obsolescence;" and Osmo A. Wiio, "Technology, Mass Communications and Values."

_____. Joint Economic Committee *Improved Statistics for Economic Growth*. Report of the Subcommittee on Economic Statistics of the Joint Economic Committee. Washington, D.C.: U.S. Government Printing Office, 1966.

_____. *Review of Federal Statistical Program*. Hearings before the Subcommittee on Economic Statistics of the Joint Economic Committee, 91st Cong., 1st sess., 1969.

U.S. Congress. Senate. *Fair Credit Reporting*. Hearings before the Committee on Banking and Currency, Senate, on S. 823, 91st Cong., 1st sess., 1969.

_____. *Federal Data Banks, Computers and the Bill of Rights*. Hearings before the Subcommittee on Constitutional Rights of the Committee on the Judiciary, Part I and Part II—Relating to Departments of Army, Defense, and Justice, Senate, 92d Cong., 1st sess., 1971.

_____. *Privacy and the Rights of Federal Employees*. Hearings before the Subcommittee on Constitutional Rights of the Committee on the Judiciary, Senate, on S. 3779, 89th Cong., 2d sess., 1966.

_____. *Privacy, the Census and Federal Questionnaires*. Hearings before the Subcommittee on Constitutional Rights of the Committee on the Judiciary, on S. 1791, 91st Cong., 1st sess., 1969.

_____. *Right of Privacy Act of 1967*. Hearings before the Subcommittee on Administrative Practice and Procedure of the Committee on the Judiciary, Senate, on S. 928, 90th Cong., 1st sess., 1967. 2 Parts.

_____. Senator Edward V. Long on Records and the Invasion of Privacy by Federal Agencies. 89th Cong., 1st sess., May 18, 1965. *Congressional Record*, III, pt. 8, 10821-10824.

Includes a reprint of Stanley P. Wagner, "Records and the Invasion of Privacy," which appeared originally in *Social Science* magazine. See references to a number of articles on privacy in magazines and scholarly journals during the 1950's.

_____. Senator John L. McClellan on Annual Electronic Surveillance Report and Wiretap Investigation, 92d Cong., 1st sess., May 10, 1971. *Congressional Record*, 117, pt. 11, 14051.

_____. Subcommittee on Constitutional Rights of the Committee on the Judiciary. "Staff Report to the Senate Subcommittee on Constitutional Rights," April 1972.

See section on privacy, pp. 3-4.

U.S. Department of Health, Education, and Welfare. *Guidebook to the U.S. Department of Health, Education, and Welfare Computer Data Files*. 1973. Forthcoming.

_____. Office of Education. *U.S.O.E. Support of Computer Projects 1965-1971*, by Lawrence P. Grayson and Janet B. Robbins. Washington, D.C.: U.S. Government Printing Office, 1972.

A directory of the Office of Education's support of approximately 500 projects involving computers for purposes of instruction, data development and analysis, information management and retrieval, administration and planning, or establishment of networks between governments or administrative sectors.

_____. Public Health Service. Health Services and Mental Health Administration. *Medical Information Systems*. Proceedings of a Conference on Medical Information Systems, January 28-30, 1970, San Francisco, California. Washington, D.C.: Department of Health, Education, and Welfare, 1970.

For a discussion of privacy, see Donald A. B. Lindberg, "A Statewide Medical Information System."

_____. National Center for Health Statistics. *Policy Statement on Release of Data for Individual Elementary Units and Related Matters*. Washington, D.C.: U.S. Department of Health, Education, and Welfare, October 1969.

Ethical, legal, technical, technological, and economic considerations governing the release of NCHS data to third parties. See Appendix A for a summary of policy statement, laws, and regulations on the confidentiality of NCHS data.

_____. National Institutes of Health. *The Institutional Guide to DHEW Policy on Protection of Human Subjects*. Washington, D.C.: U.S. Government Printing Office, December 1971.

An explanation of the policy of confidentiality of personal data collected for research projects funded by the Department of Health, Education, and Welfare. Procedures for project review and implementation of the policy are outlined.

_____. Secretary's Commission on Medical Malpractice. *Medical Malpractice*. 2 vols. Washington, D.C.: U.S. Government Printing Office, 1973.

Recommendations for solving disputes and protecting legal rights of health care providers and patients. See Chapter 4, section on Data Collection and Analysis of Medical Malpractice Claims; Chapter 5, sections on A Nationwide [Medical Malpractice] Data Gathering and Information System, and Individual Privacy; Chapter 6, sections on Access to Medical Records, The Patient's Right to Medical Information, Medical Research Involving Human Beings, and Federal Guidelines; and Chapter 8, section on What Should Be Done with the Information? Vol. 2, *Appendix*, see "Access to Medical Records," by Dennis Helfman, Glenn Jarrett, Susan Lutzker, Karen Schneider, and Peter Stein.

_____. Social and Rehabilitation Service. Children's Bureau. *Legislative Guide for Drafting Family and Juvenile Court Acts*, by William H. Sheridan. Washington, D.C.: U.S. Government Printing Office, n.d.

See sections on social, legal, and law enforcement records, and sealing of records.

_____. Youth Development and Delinquency Prevention Administration. *Legislative Guide for Drafting State-Local Programs on Juvenile Delinquency*. Washington, D.C.: Department of Health, Education, and Welfare, 1972.

Guidelines for legislation. See Section 55, "Making and Maintenance of Written Records;" Section 56, "Restrictions on Use of Records;" Section 57, "Testimonial Privilege;" Section 58, "Sealing of Records;" and Section 59, "Information from Other Agencies Concerning Child Committed to or under the Supervision of Department.

_____. Social Security Administration. *Account Number and Employer Contact Manual*. Baltimore, Md.: Social Security Administration, 1971.

_____. *Social Security Number Task Force: Report to the Commissioner*, Baltimore, Md.: U.S. Social Security Administration, 1971.

U.S. Department of Housing and Urban Development. Urban Information Systems Inter-Agency Committee. *Municipal Information Systems: The State of the Art in 1970*. Washington, D.C.: U.S. Department of Housing and Urban Development, 1970.

Report of a research project conducted by Long Island University. Prepared for the use of city officials. Details the current status of computerized municipal information systems. See Appendix C for a list of similar reports.

_____. *Urban and Regional Information Systems*. Washington, D.C.: U.S. Department of Housing and Urban Development, 1968.

U.S. Federal Trade Commission. Division of Special Projects. *Compliance with the Fair Credit Reporting Act*. Washington, D.C.: Federal Trade Commission, April 25, 1971.

U.S. General Accounting Office. Comptroller General. *Acquisition and Use of Software Products for Automatic Data Processing Systems in the Federal Government*. Washington, D.C.: General Accounting Office, 1971.

_____. *Maintenance of Automatic Data Processing Equipment in The Federal Government*. Washington, D.C.: General Accounting Office, 1968.

_____. *Report to the Congress on Opportunity for Greater Efficiency and Savings through the Use of Evaluation Techniques in the Federal Government's Computer Operations*. Washington, D.C.: U.S. General Accounting Office, 1972.

_____. *Study of the Acquisition of Peripheral Equipment for Use with Automatic Data Processing Systems*. Washington, D.C.: General Accounting Office, 1969.

U.S. Library of Congress. Congressional Research Service. Automated Information Services Section. *Modern Information Technology in the State Legislatures*. Prepared for the Joint Committee on Congressional Operations, 92d Cong., 2d sess., 1972.

One in a series of studies that review the use of data processing by state legislatures. Presents the results of a telephone survey of state systems managers and developers on (1) the development of information systems, (2) services and products developed, and (3) "problems of the prospects for mechanizing legislative support services and activities."

_____. *Resolved: That More Stringent Control Should Be Imposed upon Government Agencies Gathering Information about United States Citizens: A Collection of Excerpts and Bibliography Relating to the Intercollegiate Debate Topics, 1971-1972*. Pursuant to Public Law 88-246. 91st Cong., 1st sess. Washington, D.C.: U.S. Government Printing Office, 1971.

Published as background reading for the Intercollegiate Debate, 1971-72. From the Table of Contents:

The Right to Privacy by Samuel Warren and Louis D. Brandeis

Incursions on Privacy: Computers, Army, Wiretaps by Congressional Quarterly

Survey of Information Contained in Government Files by Senate Subcommittee on Administrative Practice and Procedure

Protection of Privacy by Helen Schaffer

Wiretapping and Our National Security by John Mitchell

The Legitimation of Electronic Eavesdropping: The Politics of "Law and Order" by Herman Schwartz

S. 782—A bill to Protect the Constitutional Right to Privacy of Federal Employees by Robert M. Foley and Harold P. Coxson

Torts—Right To Privacy—Suspension of Employee on Basis of Information in Confidential Report Obtained by Employer by David F. Simon

Privacy and Efficient Government: Proposals for a National Data Center by Harvard Law Review

The Idea of a National Data Center and the Issue of Personal Privacy by Edgar S. Dunn, Jr.

The Information Revolution and the Bill of Rights by Jerome B. Wiesner

ACE Study on Campus Unrest; Questions for Behavioral Scientists by John Walsh

Privacy in Welfare: Public Assistance and Juvenile Justice by Joel F. Handler and Margaret K. Rosenheim

Mailing Lists and the Questions of Privacy by Cornelius E. Gallagher

CONUS Revisited: The Army Covers Up by Christopher H. Pyle

Review and Analysis of Alan Westin's *Privacy and Freedom*.

Privacy: A Comparative Study of English and American Law by T. L. Yang

Selected Bibliography

_____. _____. *The Impact of Computers on Society: Selected Readings*, by Robert L. Chartrand. Washington, D.C.: Congressional Research Service, June 11, 1971.

A guide to primary source books, papers, and reports, periodical articles, anthologies, proceedings, and government documents.

U.S. Office of Science and Technology. *Privacy and Behavioral Research*. Washington, D.C.: U.S. Government Printing Office, 1967.

Proposed guidelines for the protection of personal data collected for behavioral research purposes.

U.S. President's Commission on Federal Statistics. *Federal Statistics*. 2 vols. Washington, D.C.: U.S. Government Printing Office, 1971.

Vol. 1 describes the federal statistical system and strategies for improving it. Chapter 6, "Privacy and Confidentiality," examines the extent to which present legal and technical safeguards protect individual privacy, and whether the safeguards are sufficient to promote public confidence in the federal government's collection and use of personal data. See also Chapter 7, "Findings and Recommendations on Privacy and Confidentiality." Vol. II, *Supplementary Studies*, includes Morris H. Hansen, "The Role and Feasibility of a National Data Bank, Based on Matched Records, and Alternatives;" Arthur L. Moore, "Statistics and the Problem of Privacy;" and Eleanor B. Sheldon, "Social Reporting for the 1970's."

U.S. President's Commission on Law Enforcement and Administration of Justice. *The Challenge of Crime in a Free Society*. Washington, D.C.: U.S. Government Printing Office, 1967.

University of Michigan. Institute for Social Research. "Report of the Committee on Privacy." Sidney L. Cobb, chairman. Ann Arbor, Michigan, January 1971. (Mimeographed.)

University of North Carolina at Chapel Hill. School of Pharmacy. *Proceedings - Computer-Based Information Systems in the Practice of Pharmacy*, edited by Paul D. Olejar. University of North Carolina at Chapel Hill, July 19-21, 1971.

Includes several proposals for a national drug information system.

Walsh, John. "Antipoverty R&D: Chicago Debacle Suggests Pitfalls Facing OEO." *Science*, 165:19 (1969), 1243-1245.

Ware, Willis W. *Computer Data Banks and Security Controls*. Santa Monica, Calif.: The Rand Corporation, 1970. Also presented at The Kingston Conference on Information and Personal Privacy, Queen's College, Kingston, Ontario, Canada, 21-24 May 1970.

_____. *Future Computer Technology and Its Impact*. Santa Monica, Calif.: The Rand Corporation, 1966.

Warner, Malcolm, and Michael Stone. *The Data Bank Society: Organizations, Computers, and Social Freedom*. Old Woking, Surrey, England: Unwin Brothers Limited, 1970.

Survey of governmental and private information systems in Great Britain, Europe, and the United States and their implications for personal privacy. Examines record keeping in the fields of medicine, criminal justice, finance, banking, credit, and local government.

Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review*, 4:5 (December 1890), 193-220.

Weizenbaum, Joseph. "On the Impact of the Computer on Society." *Science* 176:4035 (12 May 1972), 609-614.

Westin, Alan F., ed. *Information Technology in a Democracy*. Cambridge, Mass.: Harvard University Press, 1971.

A collection of approximately 50 papers relating to the use of information technology in the political decision-making process. Includes: Harold Black and Edward Shaw, "Detroit's Social Data Bank;" Santa Clara County, Calif., "The LOGIC Information System;" Robert R. J. Gallati, "The New York State Identification and Intelligence System;" Edward M. Brooks, "The United Planning Organization's Social Databank;" Anthony Downs, "The Political Payoffs in Urban Information Systems;" and Edgar S. Dunn, Jr., "Distinguishing Statistical and Intelligence Systems."

_____. *Privacy and Freedom*. New York: Atheneum, 1967.

A seminal work on the implications of surveillance technologies for personal privacy.

_____, and Michael A. Baker. *Databanks in a Free Society*. New York: Quadrangle Books, 1972.

The report of the National Academy of Sciences Project on Computer Databanks.

Wheeler, Stanton, ed. *On Record: Files and Dossiers in American Life*. New York: Russell Sage Foundation, 1969.

Describes record-keeping practices in American schools, credit agencies, business organizations, insurance companies, military and security agencies, public welfare systems, juvenile courts, and mental hospitals. Also includes an examination of record keeping activities of the Census Bureau and the Social Security Administration.

Wiesner, Jerome. "The Information Revolution and the Bill of Rights." *Law and Computer Technology*, 5:2 (March-April 1972).

Wilberding, Joseph C. "The Medical Information Bureau." *Transactions and Studies of the College of Physicians of Philadelphia*, 37:1 (July 1969), 43-49.

Short paper by the Executive Director of the Medical Information Bureau. Describes the need of the insurance business for an information exchange, what information is exchanged, what limitations are put on its use, and its possible future uses.

Winkler, Stanley, ed. *Computer Communication: Impacts and Implications*. The First International Conference on Computer Communication, Washington, D.C., October 24-26, 1972.

Section entitled "Data Banks and Individual Privacy" includes Bryan Niblett, "Developments in the United Kingdom;" Hans P. Gassman, "The Situation in the German Federal Republic;" and James W. Evans and Robert A. Krisely, "Integrated Municipal Information Systems—Some Potential Impacts."

Woolsey, Theodore D. "Data Banks Are Not the Answer: A Statistician's Viewpoint." *American Journal of Public Health*, 60:10 (October 1970), 1991-995.

The writer is Director, National Center for Health Statistics, Health Services and Mental Health Administration, Department of Health, Education, and Welfare.

From the Introduction:

A plea is made against overemphasis on data banks as a means of improving the availability of statistics. Specific points for the use of data banks are made.

Zastrow, Charles. "The Status of Communitywide Social Data Banks." *Welfare in Review*, 10:2 (March-April 1972), 32-36.

Findings from a study of the feasibility of a communitywide automated social information center in Dane County (Madison), Wisconsin conducted by its Social Planning Agency. See discussions of confidentiality and access to data.

**Biographical Notes on
Members of the
Secretary's Advisory Committee on
Automated Personal Data Systems**

WILLIS H. WARE. Dr. Ware is a computer scientist who joined the staff of the Rand Corporation in 1952 after five years on the staff of the Electronic Computer Project at the Institute for Advanced Study, Princeton, New Jersey, where he worked under Dr. John Von Neumann. He was the first chairman of the American Federation of Information Processing Societies and is currently Chairman of the National Security Agency Scientific Advisory Board and a member of the U.S. Air Force Scientific Advisory Board. He is the author of *Digital Computer Technology and Design* (1963), and of numerous articles on computer security and the impact of computers on society.

LAYMAN E. ALLEN. In addition to his law school appointment, Professor Allen is a Research Social Scientist at the University of Michigan Mental Health Research Institute. He has served as Editor of *Jurimetrics Journal* and Chairman of the Electronic Data Retrieval Committee of the American Bar Association. He has written on the application of symbolic logic to the law and is the inventor of games for teaching problem-solving skills.

JUAN A. ANGLERO. Señor Anglero is a career public servant of the Commonwealth of Puerto Rico. He has held posts in urban and regional planning and rural development. From 1966-1968 he was a professor-researcher with the National Institute of Development Administration, U. S. Agency for International Development (AID) Mission to Guatemala.

STANLEY J. ARONOFF. A graduate of Harvard Law School, Senator Aronoff was recently elected to his second term in the Ohio State Senate. From 1960 to 1966 he was a member of the Ohio House of Representatives.

He serves as chairman of three standing committees and has successfully sponsored legislation dealing with education, mental health and welfare, election reform, housing, and regional transportation.

WILLIAM T. BAGLEY. Elected to the California State Assembly in 1960, William Bagley is a graduate of the UCLA School of Law. He is the author of the California Public Records Act of 1968 and was chairman of the Assembly Committee on Statewide Information Policy established "to study the problem of preserving personal privacy in the computer age." The Committee published its report in March 1970.

PHILIP M. BURGESS. Professor Burgess is a student of comparative and international politics. Until recently, he was Director of The Behavioral Sciences Laboratory of the College of Social and Behavioral Sciences, Ohio State University. He served as a member of the National Technical Committee on Biomedical and Social Research of the White House Conference on Aging, 1970-71.

GERTUDE M. COX. Since retiring from the chairmanship of the Department of Statistics of North Carolina State College in 1960, Miss Cox has been active as an independent consultant in the field of biometrics. She has been President of both the American Statistical Association (1956) and the International Biometric Society (1968-1969).

K. PATRICIA CROSS. Before joining the Educational Testing Service in 1963, Dr. Cross was Dean of Students at Cornell University. A psychologist by training, she is President-Elect of the American Association for Higher Education. Her publications include *Beyond the Open Door: New Students to Higher Education* (1971) and *Explorations in Non-Traditional Study*, edited with Samuel Gould (1972).

GERALD L. DAVEY. Dr. Davey received his Ph.D. in mathematics from Stanford University in 1959. From 1968 to 1970 he was President of Credit Data Corporation, which operated the first computerized credit bureau in the United States. He has been a data-processing consultant to the Church of Jesus Christ of Latter-Day Saints since 1959.

J. TAYLOR DeWEESE. Mr. DeWeese received his law degree from the University of Pennsylvania Law School in 1973. He worked at the Office of Economic Opportunity during the summers of 1970 and 1971. He is a *magna cum laude* graduate of Grove City College; during his junior and senior year he worked part-time in the Office of Public Defender, Mercer County, Pennsylvania.

GUY H. DOBBS. Mr. Dobbs was President of his own computer software and systems consulting firm before joining the Xerox Corporation. His formal training is in engineering, computer science, mathematics and business administration. For more than a decade he has been involved in the management of software development efforts, starting with the Systems Development Corporation in 1956. Mr. Dobbs is a lecturer in information processing sciences at UCLA, a member of the Board of Trustees of the Institute for the Future, and a past member of the Computer Science and Engineering Board of the National Academy of Sciences.

ROBERT R. J. GALLATI. Dr. Gallati has been a member of the New York City Police Department for 32 years. From May 1964 to April 1973 he served, by appointment of Governor Nelson A. Rockefeller, as Director of the New York State Identification and Intelligence System (NYSIIS). Dr. Gallati holds graduate degrees in law from St. John's University and Brooklyn Law School. A leader in the field of computer-based criminal justice information systems, he was chairman of the Security and Privacy Committee of Project SEARCH (1969-1973) and a member of the F. B. I. National Crime Information Center Advisory Policy Board.

FLORENCE R. GAYNOR. Having begun her professional career as a nurse, Florence Gaynor was recently appointed Executive Director of Martland Hospital, the largest teaching hospital in the United States. Before that she had served as Executive Director of Sydenham Hospital in New York City and as a member of the faculty of Albert Einstein College of Medicine.

JOHN L. GENTILE. Before assuming his present position, Mr. Gentile served for four years as Director of the Illinois Department of Finance and was President of the National Association for State Information Systems. He is the Project Director of the Illinois Project of the IBM Security Study Center.

FRANCES GROMMERS. A physician, Dr. Grommers has had formal training in systems analysis, computer technology, operations research, and management techniques. Her research, consultation, and teaching have been concerned with the application of systems and computer technology to health problems. She is a consultant to the National Institutes of Health, companies, and other institutions active in these fields.

JANE L. HARDAWAY. Mrs. Hardaway is the only woman appointed to head a cabinet department in the Tennessee State government by Governor Winfield Dunn. As Assistant Commissioner of Personnel, she directed the implemen-

tation of a computer system designed to match qualified applicants with vacancies. In the summer of 1972, Mrs. Hardaway eliminated the requirement to supply information about arrests without conviction from all applications for State government employment in Tennessee. She is now engaged in developing a computer-based State Employees Information System to provide management information to all agencies and departments of the State government.

JAMES C. IMPARA. Dr. Impara has been on the staff of the Florida Department of Education since 1966. He has had broad experience in the design and execution of surveys and evaluations in the field of education.

PATRICIA J. LANPHERE. Mrs. Lanphere is a social worker by training. Her entire professional experience has been with the Oklahoma Department of Institutions, Social and Rehabilitative Services, starting in 1947. She helped design and implement Oklahoma's Case Information System that computerized all of the Department's public assistance and social service caseloads.

ARTHUR R. MILLER. A nationally recognized expert on the law of civil procedure, Professor Miller recently joined the faculty of Harvard Law School where, as a student, he was on the Harvard Law Review. He is the author of *The Assault on Privacy: Computers, Data Banks, and Dossiers* (1971). He has served as a member of the Panel on Legal Aspects of Information Systems, Committee on Scientific and Technical Information (COSATI); the Special Decennial Census Review Committee of the Department of Commerce; and the National Advisory Panel of the National Academy of Sciences Project on Computer Databanks. He is currently Chairman of the Security and Privacy Council of the Massachusetts Criminal History Systems Board.

DON M. MUCHMORE. Mr. Muchmore is both Senior Vice President of California Federal Savings and Loan Association and Chairman of the Board of Opinion Research of California and its affiliated polling, survey and research firms. He has been Deputy Director of Finance for the State of California and Vice Chancellor of the California State Colleges. He was a member of the Special Decennial Census Review Committee of the Department of Commerce, and is Vice Chairman of the Advisory Committee on Privacy and Confidentiality of the U. S. Bureau of the Census.

JANE V. NOREEN. Miss Noreen was a senior at Henry Sibley High School, West St. Paul, Minnesota, when appointed to the Committee. She is now an undergraduate at the University of Minnesota.

P. L. (ROY) SIEMILLER. Since his retirement as President of the International Association of Machinists and Aerospace Workers in 1969, Mr. Siemiller has been on loan from the AFL-CIO to the National Alliance of Businessmen. He started his career as a Journeyman Machinist and was General Vice President of the IAM for 17 years before becoming President.

RUTH S. SILVER (Mrs. Harold F.). Mrs. Silver is a housewife. She is active in cultural and charitable organizations in Denver, Colorado.

SHEILA SMYTHE. Miss Smythe has been in the health care field since 1957 when she joined the research staff of the national Blue Cross Association. Before her recent election as Vice President of Associated Hospital Service of New York (New York's Blue Cross), she was Executive Associate to the President of AHS. She is Chairman of the American National Standards Institute Task Force on Identification of Individuals and Organizations for Information Interchange.

JOSEPH WEIZENBAUM. Professor Weizenbaum is widely known for his work on ELIZA, a computer program for the study of natural language communication between man and machine. He has been a Professor of Computer Science at the Massachusetts Institute of Technology since 1967. He was a member of the MIT Committee for Privacy of Information and is currently a Fellow at the Center for Advanced Study in the Behavioral Sciences in Palo Alto, California.

DAVID B. H. MARTIN. Before being appointed as a Special Assistant to the Secretary of Health, Education, and Welfare in 1970, Mr. Martin had served as Executive Director of the Massachusetts Housing Finance Agency, Special Assistant to the Provost and Director of Governmental Relations at Yale University, Special Assistant to the Assistant Secretary for Legislation of HEW, and Legislative Assistant to U.S. Senator Leverett Saltonstall. He is a graduate of Harvard Law School and practiced law for 9 years in Boston.

CAROLE WATTS PARSONS. Miss Parsons is a political scientist specializing in comparative government and national science policy. She came to HEW from the National Academy of Sciences where she was Executive Secretary of the Advisory Committee on Problems of Census Enumeration and Staff Associate in the Division of Behavioral Sciences. Miss Parsons is Chairman of the American Political Science Association Committee on the Status of Women.

Index

- Abortion, 34
Actual damages, xxiii, 50
Adams, John Quincy, 184, 185
Administrative records, *see* Records
Advisory Commission on Intergovernmental Relations, 141
Alabama, State of, 188, 211
Alaska, State of, 34
ALERT System, 234n.
American Association of Motor Vehicle Administrators, 207
American Federation of Information Processing Societies (AFIPS), 29n., 289
American Medical Association, 251
American National Standards Institute (ANSI), 122n.
Anonymity, *see* Confidentiality
ANSI standard identification format, xxxiii, 122n., 140
American Philosophical Society, 178n., 182
American Statistical Association, 188-189
Archives, *see* Records
Arrests, *see* Records
Asia Minor, 1
Association for Computing Machinery, 42
Attorney General of the United States, 105, 138, 189, 236, 241, 242 ff., 261
Audit trails, xxv, 56, 62, 216
Automated personal data systems, 13, 14, 28; access to data in, ix, 19, 55-56, 60-63, 94-95, 96, 98, 121, 216; administrative, xxiv-xxvii, 48, 51, 53-64, 73, 78-87, 215-220, 247; administrative used for statistical reporting or research, xxi, xxvii, xxix, 49, 59, 78-87; definition of, 49-50; employees of, xxiv, 54-55, 57, 98; establishment of, 51-52, 138-139; for statistical-reporting and research, xxi, xxix-xxxi, 26, 48, 50, 54, 59, 89-102; fragility of, 14-15, 168; managers of, 13, 44-46, 80, 98, 216; multijurisdictional, 21, 54, 98, 169, 214-215, 216-217, 219, 222; regulation of, 42-43; research uses of, 78-87, 89-102; safeguards for, xx, xxi, xxiv-xxxi, xxxiii, 43-45, 49, 50, 53-64, 73, 85-87, 97-102, 112, 121, 136, 215-220, 247, 296; secret, 41 social impact of, ix, xx, 12-30, 140-141, 167-168; *see also* Record keeping
Automobile Manufacturers Association, 214
Baden-Württemberg, State of, 169
Bank records, *see* Records
"Bank Secrecy Act," 21n., 120

Bavaria, State of, 169
 Billing systems, 13
 Bill of Rights, 34, 241, 242
 Birth records, *see* Records
 Blackmail, 19
 Blue Cross, 283
 British Computer Society, 174
 Burney, L. E., 282

California Bankers Association, 21n.
 California Department of Corrections, 253
 California Department of Education, 251
 California State of, 34, 226
 Canada, 174-175
 Canadian Task Force on Privacy and Computers, x, 175
 Canal Zone, 208
 Census Act, 89, 90n., 92, 104, 200-201
 Census of Business and Manufactures, 82, 184n.
 Census of Population, 4, 93; of 1790, 180-181; of 1800, 182-183; of 1810, 183-184; of 1820, 184-185; of 1830, 185-186; of 1840, 186-189; of 1850, 189-191; of 1860, 191-192; of 1870, 192-193; of 1880, 194-197; of 1890, 197-198
 Census tract data, 293
 Check-digit, 110n., 114
 China, 1
 Civil remedies, xxi, xxiii, xxiv, 44, 50, 55, 136
 Civil Rights Act of 1964, 270
 Class actions, xxiii, 50
 Codes of ethics for data-processing personnel, 55, 141
 Code of Fair Information Practice, xx, xxiii, xxix, 41-44, 50, 52, 55, 59, 69, 75, 95-96, 100, 136; and the Fair Credit Reporting Act, 66-71; and the Freedom of Information Act, 64-66; basic principles of, 41-42; violations of, 50
 Collective bargaining, 50
 Colvin, James B., 183
 Committee on Privacy (U.K.), 173-174
 Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment,

and Rehabilitation Act of 1970, 105, 280
 Comprehensive Drug Abuse Prevention and Control Act of 1970, 280
 Comptroller of the Currency, 69n.
 Compulsory legal process, xix, xxi, xxvi, xxxi, xxxii, 63, 67, 80, 91, 214-215; protection from, 96-106, 102-106, 137
 Computer-accessible files, 23, 50, 51, 56; definition, 49
 Computer programs, 13, 14, 21n., 22
 Computers, effects on record keeping practice, xix, 8, 12-30; and telecommunications, v, viii;
 Computer security, *see* Automated personal data systems
 Confidentiality, 6; of census data, 4, 7n., 178-201; of clinical information, 280; of Social Security data, 274-275; of statistical-reporting and research data, xxxi, 87, 91-94, 100; of the Social Security number, xxxv, 131, 133; of third-party recommendations, 60-61; statutes, 89, 90n., 92, 104, 200-201, 279-280; under Public Health Service Act, 279-280
 Connecticut Academy of Arts and Sciences, 182
 Conseil d'Etat, 171
 Consumer-reporting industry, 66-71
 Contraception, 34
 Cooley's anemia, 278
 Correctional Decisions Information Project (CDIP), 247-257
 Council of State Governments, 141
 Cour de Cassation, 171-172
 Courts, and privacy rights, 34, 36-38, 43, 44
 Cox, Samuel S., 194, 195
 Cox, Tench, 184
 Credit bureaus, *see* Consumer-reporting industry
 Credit cards, 27, 131
 Credit records, *see* Records
 Criminal penalties, xxi, xxiii, 44, 50, 104, 136
 Criminal history files, *see* Records
 Criminal justice information systems, 222-246

Currency and Foreign Transactions Reporting Act, *see* "Bank Secrecy Act"

Data, *see* Personal data
 Data collection requirements, 52
 imposed by formal rule making, 139
 Data files, documentation of, xxviii, 86, 95, 99
 Data Inspectorate (Sweden), 170, 171
 Data processing, xix, 12, 13-15, 22-23, 49, 57, 169; *see also* Automated personal data systems
 Data Protection Act (Hesse), 168-170
 Data Protection Commissioner (Hesse), 169-170
 Data subjects, *see* Rights of individuals
 Data systems, *see* Automated personal data system
 Daunt, Jerome, 231, 239
 Death records, *see* Records
 DeBow, James D.B., 191, 198
 Délégue à l'Informatique, 171
 Department of Communications (Canada), 174
 Department of Justice (Canada), 174
 Department of Justice (France), 171
 Direct Mail Advertising Association (DMAA), 73, 291-292, 295
 District of Columbia, 207
 Documentation, *see* Data files
 Domesday Book, 2
 Dossiers, *see* Intelligence records
 "Dragnet" effect, 16-17, 57, 212-213
 Driver licenses, *see* Records
 Drug Abuse Office and Treatment Act of 1972, 105-106
 Due process, vi, 61, 75

Education Professions Development Act, 262-263
 Elementary and Secondary Education Act, 261
 Employment records, *see* Records
 Error measurement, xxviii, 83, 86
 Ervin, Senator Sam J., Jr., 108, 238
 Evaluation research, 91-92, 94, 134
 Executive Order 9397, 116-117
 Executive Order 10561, 286
 Executive Order 11246, 269
 Expungement rules, 51, 57, 217

Fair Credit Reporting Act, xxvii, 37, 66-71, 137
 Federal Bureau of Investigation (FBI), 17-18, 216, 226, 229-235, 236, 245, 275
 Federal Coal Mine Health and Safety Act of 1969, 264-265
 Federal Food, Drug, and Cosmetic Act, 264
 Federal Old-Age, Survivors and Disability Insurance Benefits (OASDI), 265-266
Federal Register, 58, 101
 Federal Reports Act, 35, 84, 258, 270-272
 Federal Reserve Board, 69n.
 Federal Reserve System, 69n.
Federalist Papers, 179
 Fingerprinting, 17, 24, 129, 226
 Florida, State of, 226, 232
 France, 1, 14, 171-172
 Frankfurter, Justice Felix, 242
 Freedom of Information Act, xxvii, xxxii, 35-36, 64-66, 91, 137, 138, 258, 281; discretionary exemptions, 65-66, 103, 273-274

Gallatin, Albert, 183-184
 Gannett, Henry, 194
 Garfield, James A., 192, 193, 194
 General Accounting Office (GAO), 90n.
 General Education Provisions Act, 262-263, 283-284
 General Services Administration (GSA), 283, 286
 Georgia, State of, 188
 German Federal Republic, 168-170
 Great Britain, 173-174, 215, 289
Gregory v. Litton Systems, 243
 Guam, 207

Hamburg, State of, 169
 Hammurabi, Code of, 2
 Health care delivery, 9, 24-28
 Health Insurance for the Aged, *see* Medicare
 Health Services & Mental Health Administration (HSMHA), 258n., 264, 282
 Hollerith, Herman, 196-197
 Hoover, Herbert, 201
 Hruska, Senator Roman, 240

- IBM Personal Identification Code, 210
 Immigration and Nationality Act, 275
 Inca civilization, 1-2
 Income-tax returns, *see* Records
 India, 1
 Informed consent, xxii, xxvi, xxvii, xxix, xxxiv-xxxv, 53, 56, 59, 65-66, 80-82, 85, 93, 98, 104, 131, 137, 138
 Injunctions, xxi, 50, 136
 Insurance, *see* Records
 Integrated municipal information systems (IMIS), 20, 43n., 237-238
 Intelligence records, *see* Records
 Internal Revenue Act, 266
 Internal Revenue Code, 118
 Internal Revenue Service, 82, 83, 114, 117, 120, 131, 232, 259, 266, 268
 Investigative-reporting companies, *see* Consumer-reporting industry
 Irving, John F.X., 230-231
- Jackson, Andrew, 188
 Jefferson, Thomas, 181, 183
Joint Anti-Fascist Refugee Committee v. McGrath, 242
- Kennedy, Joseph C.G., 190-191; 192
 King John of England, 3
 King's Remembrancer, 2
 Knisely, Robert, 237-238
 Kremel, Franklin M., 214
- Labor unions, 50
Lamont v. Commissioner of Motor Vehicles, 290n., 297
 Land surveys, 2
 Law Enforcement Assistance Administration (LEAA), 222-225, 227 ff.
 Lear, Tobias, 181
 Leonard, Jerris, 229
Letters close, 3
Letters patent, 3
 Licenses, *see* Records
 Liquidated damages, xxiii, 50
 Little Sisters of the Poor, 293
 Local governments, xxiii, 21, 50, 58; using SSN, 125
 Longitudinal studies, 92
 Louisiana, State of, 188
 Lower Saxony, State of, 169
- Machine intelligence, 22
 Madison, James, 179-180, 183
 Magdalenian period, 1
 Magna Carta, 2
 Mailing lists, 71-73, 288-297
 Mail Preference Service, 73, 291-292, 296
 Management information systems, ix, 6, 23, 82
 Maryland Psychiatric Case Register, 218
 Massachusetts, Commonwealth of, 188
 Mass media, 168
 Medical records, *see* Records
 Medicare, v, 119, 266
 Mercer County (N.J.), 89-90
 Mesopotamia, 2
 Michigan, State of, 226
 Microfilm, 49, 50
 Mitchell, John N., 223, 230, 231
 Mitchill, Samuel Latham, 184
 Morrill, Justin, 194
 Motor Vehicles Departments, State, 15-17, 18, 73, 81, 203, 202-221
 Multijurisdictional systems, *see* Automated personal data systems
 Musée des Antiquités Nationales, 1
 Mutuality, Concept of xx, 40-42, 60, 65
- National Academy of Sciences, 244;
 Project on Computer Databanks, x, 112n.
 National Center for Health Statistics, 94, 264, 281, 282
 National Commission on Individual Rights, 240
 National Conference of Commissioners on Uniform State Laws, 141
 National Conference of State Legislative Leaders, 141
 National Crime Information Center (NCIC), 17-18, 216, 226-227, 229, 232-235, 236 ff.
 National Driver Register, 15-17, 18, 120, 202-221
 National Governors Conference, 141
 National Health Surveys, 104, 263-264, 279
 National Highway Traffic Safety Administration, 203
 National Institute of Education (DHEW), 258n., 259n., 260

- National Institute of Law Enforcement and Criminal Justice, 223
 National Institute of Mental Health (DHEW), 134, 282
 National Institutes of Health (DHEW) 258n., 259n., 260
 National League of Cities, 237
 National Legislative Conference, 141
 National population register, 111
 National statistical data center, 91
 New York Historical Society, 189
 New York State Identification and Intelligence System (NYSIIS), 225-226, 227, 236
- Older Americans Act of 1965, 267
 Ombudsman, 42
 Organic Act of 1867, 261
 Organized Crime Control Act of 1970, 241
- Palfrey, John Gorham, 189
 Parish registers, 2
 Peer review, 83, 84, 86, 94-95
 Personal data, accuracy of, xxv, xxvi, 56-57, 58, 63-64, 67, 216, 220; categories of, xxv, xxxi, 14, 58, 99; collection of, 49, 51-52, 83; completeness of, xxv, xxvi, 56-57, 58, 63-64, 69, 216, 220; definition of, 49; individual control over, 28-30, 39-42; pertinence of, xxv, xxvi, 56-57, 58, 63-64, 69, 79-81, 216, 220; sources of, 58, 61, 68, 71; timeliness of, xxv, xxvi, 56-57, 58, 63-64, 67, 216, 220; transfers of, xxiv, xxix, xxxi, 7, 53-54, 55-56, 61-62, 67-68, 97, 98-99, 101, 217-219, 266-267
- Personal-data record keeping, *see* Automated personal data systems
 Personnel records, *see* Records
 Pickering, Timothy, 182-183
 Planning, 3, 7, 9
 Pornography, 34
 Porter, Robert P., 197-198
 Postmaster General, 115, 189
 President's Commission on Law Enforcement and Administration of Justice, 222n., 223
- Privacy, and record keeping, xx, 7, 29-30, 33-42, 44, 66, 140; re-definition of, 38-42
 Professional Standards Review Organization (PSRO), 278-279
 Project SEARCH, 227-233, 240
 Public assistance payments, v, 277
 Public Health Service Act, 93, 104, 260, 261, 263-264, 278, 279-280
 Public Information Act, *See* Freedom of Information Act
 Public Notice Requirement, xxv-xxvi, xxx-xxxii, 57-58, 62, 87, 99-100, 139, 217
 Public opinion, 29, 111, 159, 168, 289
 Public records, *see* Records
 Public record statutes, 36; *see also*, Freedom of Information Act
- quipu*, 2
- Reader's Digest*, 289
 Record keepers, 1-4; technicians as, xix, 12, 22-28, 55;
 Record keeping, computer-based 7-8, 12-30; law 34-36, 53, 64-71, 225; manual xxiv, xxix, 1-7, 14, 19, 49, 53, 208, 215; principles of, xx, 6-7;
 Record-keeping organizations, xxiii, xxiv-xxvi, xxviii, xxix-xxxii, 21n., 38-42, 44-46, 53-64, 78-79, 82-85, 86, 93, 97
 Record-keeping systems, *see* Automated personal data systems
 Record linkage, xxii, xxxiii, 20-21, 23, 24, 108, 109, 111, 121, 140, 167
 Record-matching, *see* Record linkage
 Records, administrative, xix, 3, 4, 5, 6, 9, 21, 23, 25, 26-27, 292; anonymous sources of, 61; archival, 50, 57; arrest, 18, 67; birth, 2, 5, 292; credit, 9, 66-71, 83n., 224, 292; criminal history, 17-19, 67, 222-242; death, 2; driver licensing, 15-17, 18, 72, 120, 202-221; financial, 5, 7, 8, 28, 49, 65, 67, 75, 89, 120; insurance, 8, 66, 68, 168, 224; intelligence, xix, xxi, 3, 5, 6, 9, 20-21, 48n., 65, 74-75; investigative, xxvii, 68-70, 138; juve-

nile court, 83n.; marriage, 2, 292; medical, xxvii, 24-28, 49, 60, 65, 70, 106, 133-134, 138, 224, 285; national security, 75; occupational licensing, 18, 60, 68, 75; personnel and employment, 6, 60, 65, 66, 68, 168; public, 1-4, 5, 6, 7, 21n., 80, 292; school, 5, 7, 9, 19, 28, 60, 72, 83n., 168, 292; statistical, xix, 4, 6, 9, 25, 26; tax, 2, 7, 67, 82, 168; types of, 5-6; welfare, v-vi, 9, 83n., 84-85, 224; *see also* public assistance payments.

Registration, of data banks, 42-43; student, 29

Regulation of data banks, 42-43

Regulatory agencies, 28, 43n., 69

Reorganization Plan No. 1 (1953), 260

Rheinland-Pfalz, State of, 169

Richardson, Elliot L., viii, 108

Rights of individuals, xxvi, xxxi, 59-64, 67-69, 101-102, 103, 121-122, 137-138, 217-218; regarding the SSN, 125-126, 127, 137

R.L. Polk & Co., 293

Roderick, Donald, 239

Roman Empire, 2, 4

Russell, Archibald, 189, 190

Safe Streets Act, 240

Safeguards requirements, applied by formal rule making, xxiii, xxix, 50, 66, 96, 138; applied to correctional decision-making process, 247; applied to National Driver Register, 215-220; costs, of, 44-46; exemptions from, xx, 43-45, 52-53, 56, 60-61, 65-66, 70, 73, 75, 100, 138, 218, 295-297; for administrative personal data systems, xxi, xxiv-xxvii, 49, 50, 53-64, 73, 85n., 86-87, 136, 215-220, 296; for statistical-reporting and research applications of administrative personal data systems, xxi, xxvii, xxix, 49, 59, 85-87; for statistical-reporting and research systems, xxi, xxix-xxxi, 49, 50, 54, 59, 97-102, 136; monitoring the effects of, 141.

Safety Management Institute, 215

Scandinavia, 4

Schleswig-Holstein, State of, 169

School records, *see* Records

Seaton, Charles W., 196

Secretary of Defense, 120

Secretary of Health, Education, and Welfare, iii, vii, viii, xix, xxxv, 104, 105, 108, 128, 129, 136, 140, 142-143, 261, 263, 264, 265, 266

Secretary of Labor, 269

Secretary of State, 182, 184, 187, 189

Secretary of the Treasury, 118, 183, 267, 268

Secretary of Transportation, 206

Shattuck, Lemuel, 189, 190

Social Security payments, 8

Social Security Account Number, *see* Social Security number

Social Security Act of 1935, 93, 106, 113, 114-115, 131, 260, 265-266, 267-268, 274-275, 276-277, 278-279, 281, 283; as amended in 1965, 119; as amended in 1972, xxxv, 126, 127, 128-129, 139, 278.

Social Security Administration, 44-45, 83, 112, 113, 114, 117, 118, 119, 120, 126, 127, 128, 133, 134, 135, 139-140, 208, 209, 210, 259n.; *see also*, Social Security Board

Social Security Board, 115, 116-117, *see also*, Social Security Administration

Social Security Claims Manual, 283

Social Security Handbook, 283

Social Security number (SSN), xix, xxi, 23, 27, 49, 81, 203, 204, 205, 210, 211, 286; and safeguards for automated personal data systems, xxxiii, 112, 121, 124; as a standard universal identifier, xxxii, 112-114, 121-122, 129, 210; as a password, 131-132; as driver license number, 213; as taxpayer's identification number, 117-118; authority granted by Section 137 of P.L. 92-603 (1972), 129; confidentiality of, 131, 133; Federal program uses, 116-121, 124, 126, 132, 137, 139-140; history of, 114-122; multiple number problem, 112, 126-127; ninth-grade enumeration, xxii, xxxiv, 119, 127, 139; non-data-processing uses, xxii, xxxv, 134-135; non-Federal program uses,

130; pocketbook numbers, 112n.; protections against unauthorized uses, 137; recommendations on, xxi, xxxiii-xxxv, 125-135.

"SSN services," xxxv, 139; constraints on, 132-134; definition of, 132; in aid of research, 133.

Social Security Number Task Force, xxii, 108, 126, 127, 128, 132-134

Soundex system, 209-210

South Carolina, State of, 34

Standard Nomenclature of Diseases and Operations, 251

Standard universal identifier (SUI), xxi; xxxii; 23-24, 27, 28; 108-114; 121; 129-130; 140; *de facto*, 112-113, 121, 126, 127, 130.

Stark v. Connally, 21n.

State constitutions, 34

State governments, xxiii, 21, 50, 58, 96; using the SSN, 125

Statistical disclosure, xxxii, 103

Statistical records, *see* Records

Statistical reporting, 26; systems, 89-102; uses of administrative automated personal data systems, 78-87

Statistical stereotyping, 26

Subpoenas, *see* compulsory legal process

Sumer, 2

Surgeon General, 282

Surveillance, xxii, 24-28, 223-224

Sweden, 170-171, 215

Swedish Committee on automated personal data systems, x, 170-171

Tally sticks, 1

Taxpayer's identification number, *see* Social Security number (SSN)

Tax records, *see* Records

Technology assessment, 45-46

Telephone directory, 292, 293, 294

Thomas, District Judge Edward B., 199

Title 13 U.S.C. (Census Act), 89, 90n., 92, 104, 200-201

Title 18 U.S.C., 259, 276

Trade secrets, 65, 273

Unemployment compensation, 115

Unfair information practice, *see* Code of Fair Information Practice

U.S. Bureau of the Budget, 116; *see also* U.S. Office of Management and Budget

U.S. Bureau of Customs, 232

U.S. Bureau of the Census, 73, 89, 90, 94, 179, 199-201, 295

U.S. Civil Aeronautics Board, 69n.

U.S. Civil Service Commission, 116-117, 119, 259, 272, 284-287

U.S. Commission of Education, 261, 262

U.S. Commissioner of Internal Revenue, 115, 118

U.S. Commissioner of Social Security, 119, 127, 128

U.S. Commissioner on Aging, 267

U.S. Congress, xxxiii, 69, 90n., 120, 124, 125, 179ff., 214, 219, 234n., 245, 246, 259, 268; legislative proposals to, 136-138, 243-245, 246.

U.S. Constitution, Article I, Sec. 2, 178, 179; First Amendment, 34, 241; Third Amendment, 34; Fourth Amendment, 34; Fifth Amendment, 34, 241, 242; Ninth Amendment, 34; Fourteenth Amendment, 241-242.

U.S. Department of Commerce, 289

U.S. Department of Health, Education, and Welfare, 24-28, 44-45, 94, 106, 138-143; Administration on Aging, 259n., 267; Office for Civil Rights, 259n., 269; Office of Child Development (OCD), 259n., 268; Office of Human Development, 259n.; Office of the Secretary (OS), 142-143, 259n.; Office of Youth Development (OYD), 259n.; record-keeping law, 258-287; Public Information Regulation, 273-274; *see also* Health Services and Mental Health Administration; National Center for Health Statistics; National Institute of Education; National Institutes of Health; National Institute of Mental Health.

U.S. Department of Housing and Urban Development, 237

U.S. Department of Justice, 222, 234, 245; *see also*, Federal Bureau of Investigation

U.S. Department of Labor, 270

U.S. Department of State, 183, 188

U.S. Department of Transportation,
15-17, 120, 203ff

U.S. Department of the Treasury, 114,
118, 120, 186, 232; *see also*, Internal
Revenue Service

U.S. Federal Trade Commission, 69n.,
138

U.S. Food and Drug Administration
(FDA), 258n., 259n., 281

U.S. Immigration and Naturalization Ser-
vice, 232

U.S. Interstate Commerce Commission,
69n.

U.S. Office of Education, 259-259n.,
283

U.S. Office of Federal Contract Com-
pliance, 269

U.S. Office of Management and Budget,
141, 270-271; 286; *see also*, U.S.
Bureau of the Budget

U.S. Postal Service, 72, 73, 289-290, 295

U.S. Public Health Service, 119, 258n.,
259n.

U.S. Secret Service, 232, 275

U.S. Social & Rehabilitation Service
(DHEW), 120, 259, 281

U.S. Veterans Administration, 119; *see*

also General Accounting Office;
General Services Administration
U.S. v. Moriarty, 180, 199-200

Van Buren, Martin, 187

Velde, Richard W., 228

Venereal Disease Prevention and Control
Program, 278

Virgin Islands, 208

Virginia, Commonwealth of, 188, 211

Wagner, Jacob, 183

Walker, Francis Amasa, 193-194, 196

Washington, George, 181

Weaver, William A., 188

Weisner, Jerome, 225

Welfare records, *see* Records

Wiretapping, 29, 172

Wright, Carroll D., 198

Younger Committee (U.K.), 173-174,
289

Younger, Rt. Hon. Kenneth, 173n.

U.S. GPO: 1977 O-370-170

United States, Dept. of
Health, Education, and
Welfare

Records, computers, and the
rights of citizens