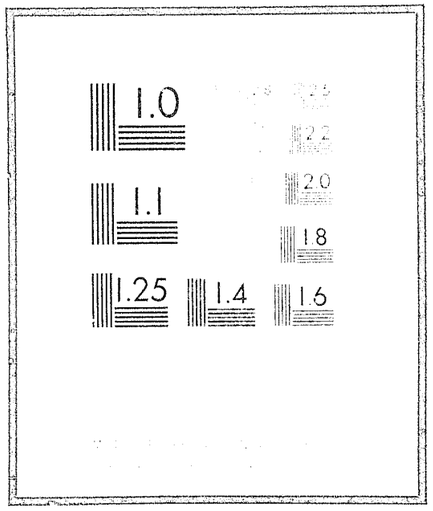
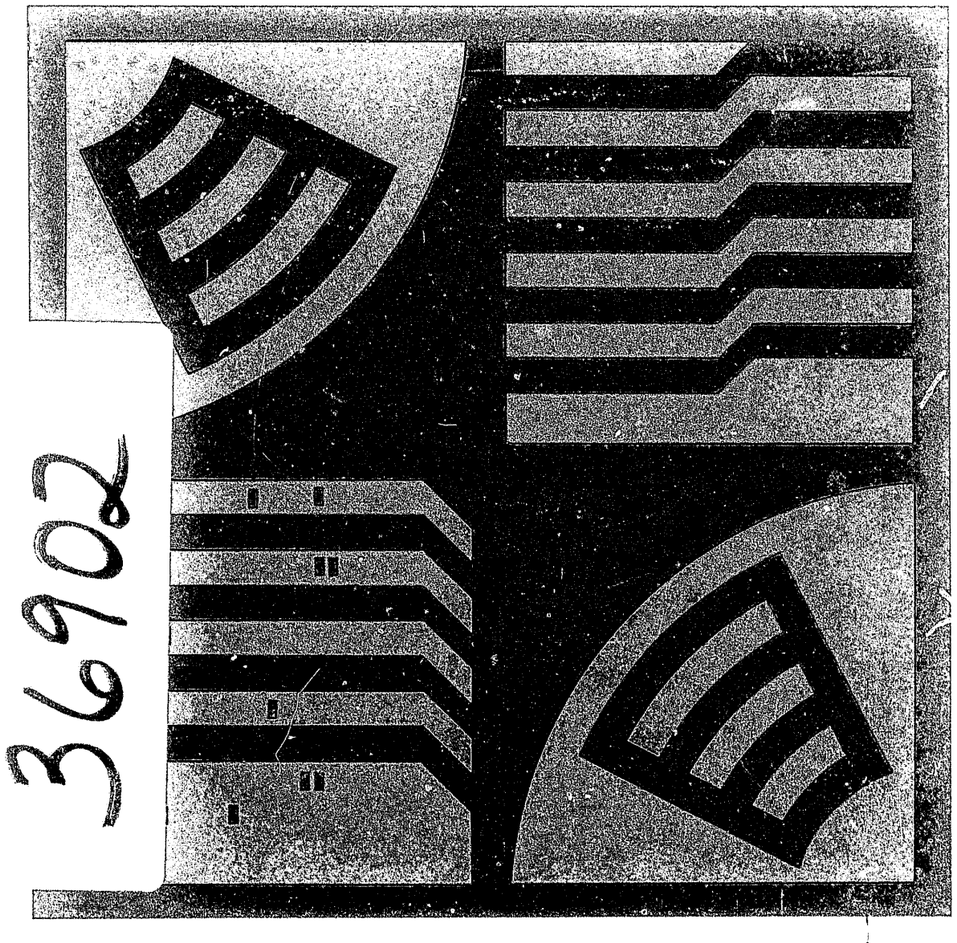


PRIVACY, A PUBLIC CONCERN:

A RESOURCE DOCUMENT

based on the proceedings of a Seminar on Privacy sponsored by The Domestic Council Committee on the Right of Privacy and The Council of State Governments



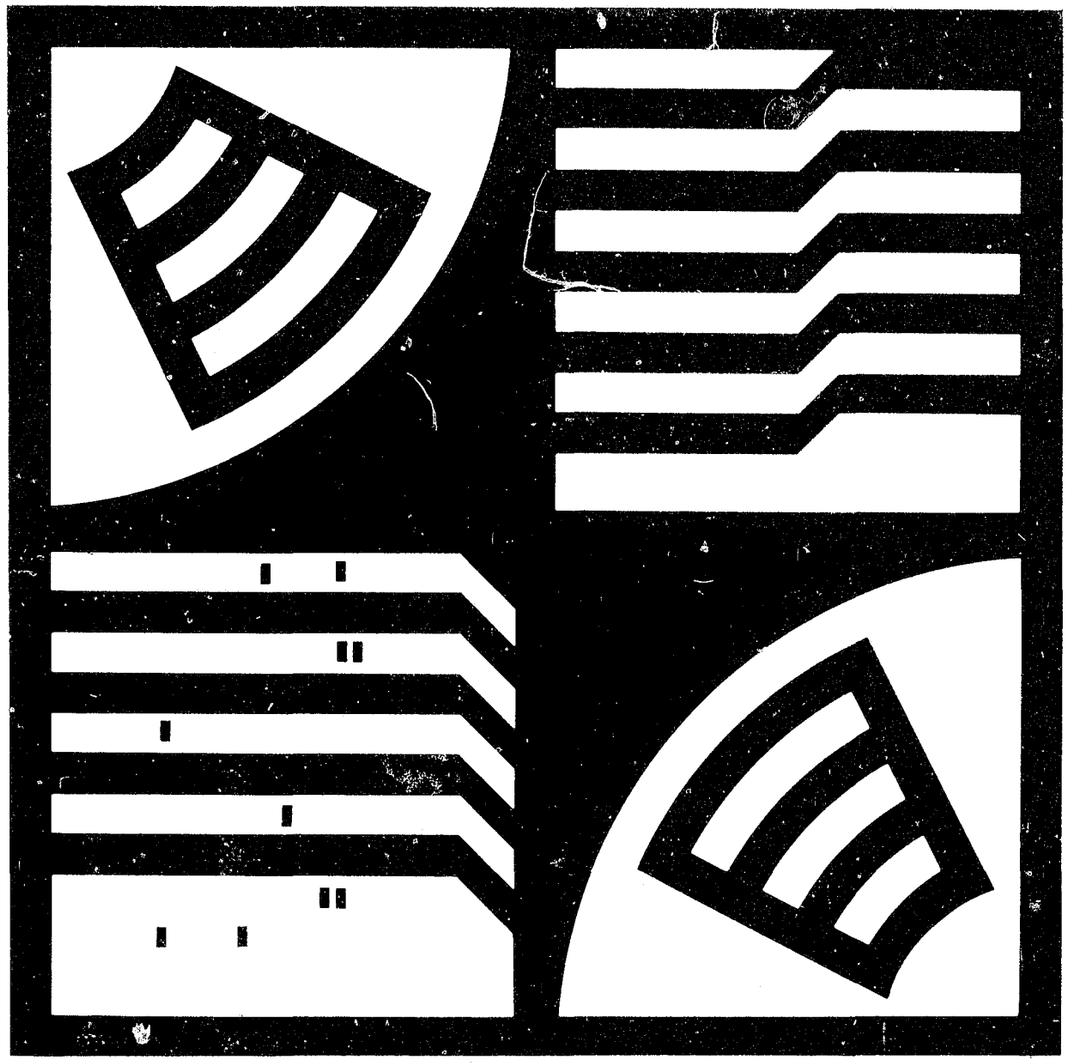
PRIVACY, A PUBLIC CONCERN:

A RESOURCE DOCUMENT

based on the proceedings of a Seminar on Privacy sponsored by The Domestic Council Committee on the Right of Privacy and The Council of State Governments

Edited by Kent S. Larsen

August 1975



For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402 - Price $3.20

CONTENTS

FOREWORD

Materials in this resource document were compiled for use in a Washington seminar held in December, 1974, co-sponsored by the Domestic Council Committee on the Right of Privacy and the Council of State Governments. The seminar was directed to the interests of State and local government and was intended to explore the alternatives for intergovernmental strategies in privacy protection policy formulation and implementation. We were motivated to join in this seminar because of the increasing interest in personal privacy at the State and local level, and we desired to share experience and insights gained by the Federal government in the development of the Privacy Act of 1974 (P.L. 93–579), signed into law on December 31, 1974. That Act pertains mainly to the practices of Federal agencies, but its privacy principles regarding information management are of relevance to State and local government as well.

The matter of personal privacy is one important facet of broader questions of information law and policy. Our society grows in the need for personal information in order to provide the comprehensive services that government and the private sector seek to make available. The process is not simple, of balancing the need for information against the individual's desire to limit the quantity of information about himself that may become public, but it is a task that must be accomplished to insure the responsible management and operation of programs that are dependant upon information about people.

The original seminar materials have been updated and expanded in this document and are designed to provide an overview of the breadth and depth of questions of informational privacy, and to display some of the complexities in information regulation and management. They explore representative areas of information requirements, displaying many of the competing interests that must be balanced regarding the collection, use and dissemination of personal information. It is unwise for any government to enter upon the regulation of information processing without careful study of the potential impact of

such regulation on the business practices of government itself, and upon the private sector.

Relevant portions of these materials will be useful to replicate a conference, workshop or seminar, such as we held in Washington, or to provide a foundation for research and inquiry in the development of privacy protection policy. We make this document available in the hope it will help others to find a useful entry-point into the matter of personal information privacy, though we know it is by no means exhaustive or complete. The bibliography included suggests other sources for research into the many complex issues of information management. From time to time, as the Federal government gains experience in the implementation of the Privacy Act, sharing what is learned hopefully can make it easier for others to minimize difficulties and decrease the costs of program development.

QUINCY RODGERS
EXECUTIVE DIRECTOR

GEORGE B. TRUBOW
GENERAL COUNSEL
(SEMINAR CO-CHAIRMAN)

THE DOMESTIC COUNCIL COMMITTEE
ON THE RIGHT OF PRIVACY

CHAPTER 1

INTRODUCTION

Until recently, most Americans probably did not consider their right to privacy a significant issue. Many were unconcerned about whether governmental or private organizations paid any attention to personal privacy, and they were confident that their own privacy was indeed under proper safeguard.

Today, while it may not yet have achieved universal popularity, privacy appears to be on the way to becoming a household concern. Dramatic progress in the development of information and record-keeping technology, particularly during the last decade, has contributed significantly to this relatively new concern. Information about virtually every aspect of an individual's life is now compiled and maintained as a matter of course by numerous governmental and private agencies. In many cases, however, safeguards against privacy invasion have lagged behind the mushrooming technological development. (See Appendix I for a brief sketch on the historical background of privacy protection and Appendix II for a glossary of frequently encountered terms.)

Individuals within the Federal government, increasingly aware of these concerns, recognized the emerging need and took steps to meet it. The President, in February of 1974, established the cabinet-level Domestic Council Committee on the Right of Privacy to consider and recommend prompt action to assure a proper balance between the individual right of personal privacy and the necessary practices of public and private organizations in accumulating and managing information about people. At the same time, individuals within State and local government experienced similar concerns, began searching for answers, and formulated legislative initiatives within their own governmental systems. Knowledge of these activities and developments began accumulating, principally in the offices of the Council of State Governments.

This mutuality of concern seemed almost naturally to spawn the idea of a possible coordinated or at

least a cooperative Federal-State-local effort. Thus, in the early fall of 1974 the concept of a Privacy Seminar evolved, and the Domestic Council Committee on the Right of Privacy combined with the Council of State Governments in joint sponsorship. Although time was short, the staff recognized that the most favorable place and date for the seminar would be Washington, D. C., in mid-December—and so agreed despite constraints imposed by that short planning and preparation time. This schedule recognized the advantage of introducing various privacy concepts to attendees in advance of the openings of most State legislatures and assemblies. It also insured a better attendance than if it had been held later.

Early in the planning it was determined that the seminar should provide an opportunity for State and local officials to exchange views on approaches to providing personal privacy protection at the State and local levels of government—an opportunity not only to discover what was needed and wanted, but also what might work. In a word, the seminar could provide a strategy for action.

Given that overall objective, the staff had the tasks of establishing the specific subjects to be covered and deciding on the most effective vehicle to accomplish that coverage. After considerable exploration and discussion, staff members agreed that three separate main sessions would be held, one each on criminal justice information systems, State and local government data banks, and employee records. As a vehicle for stimulating discussion and thought in these areas, the staff developed the concept of a mock legislative hearing, including a chairman and various witnesses. Other discussion subjects, covered through different approaches, included consumer privacy interests, privacy cost implications, and privacy strategy for the future. (The final program agenda of the Privacy Seminar is Appendix III.)

In the selection of attendees, the staff considered it important to include not only those acquainted with and interested in privacy, but also those in professional positions of the type that would provide an opportunity for action. The staff also wanted to balance representation across the country and from various levels of government—State legislators, State administrators and local government administrators. Response to the invitation was gratifying, with over 150 participants from 37 States and the District of Columbia. (A list of attendees is included as Appendix IV.)

To encourage attendees to prepare for the seminar, a workbook containing carefully selected materials was mailed, and participants had several days to get acquainted with its contents—articles on privacy, issue papers, and various samples of model, proposed and enacted legislation. (These materials are included in this compilation along with additional items that will bring the reader up to date and round out the basic resource value of the document.) An extensive reading list of significant literature on the privacy question was provided each participant at the outset of the seminar (see Appendix V for an updated version), and a convenient resource center was established near the seminar meeting rooms, which included works from the reading list as well as other materials of interest.

The following chapters summarize the various sessions of the Seminar and its conclusions. Four chapters contain transcript summaries of the various sessions and, as appropriate, issue papers and sample legislation on the subjects. There are also chapters on the luncheon speeches, on systems cost and on a strategy for the future.

Included as appendixes are four background articles on privacy, several samples of additional State legislation of interest, and the Federal Privacy Act of 1974 (because of its high interest value) along with a commentary.

CHAPTER 2

CRIMINAL JUSTICE INFORMATION

Not too surprisingly, the mock legisiative session on criminal justice information attracted the greatest Seminar participant interest.

Chaired by Attorney General Robert Quinn of Massachusetts, the committee consisted of State Senator William Ray of Alaska, Ms. Helen Lesain of the Law Enforcement Assistance Administration, and Deputy Attorney General Morris Solomon of Pennsylvania.

The materials mailed out to each pre-registered Seminar participant included the following issue paper, which has been edited for inclusion here:

ISSUE PAPER

PRIVACY CONSIDERATIONS FOR CRIMINAL JUSTICE INFORMATION LEGISLATION

A number of issues should be addressed in considering any criminal justice information legislation relating to the protection of privacy. The following is an attempt to delineate some of those issues, without suggesting specific resolution of them.

SCOPE: The first issue to be addressed is the scope of such legislation. What agencies should it cover? What types of records? What aspects of the records?

Agencies: While law enforcement agencies are the primary collectors of criminal justice information, they are not the sole users of it. The extent to which these agencies should be covered by legislation dealing with criminal justice information is a fundamental issue, particularly with respect to the courts because they are a separate and equal branch of government.

Information covered. Legislation dealing with criminal justice information could be limited solely to notations of factual data—rap sheets. It could, however, cover a much broader range—intelligence, criminal investigations, prison, probation and parole records, and various court records. Deciding which records to cover precedes choices of methods of regulation.

Aspects of coverage. No matter which records are covered, it will be necessary to determine which aspects will be regulated in any legislation. Should regulation hinge on the collection of the records or only their use? Should it deal with dissemination and exchange outside the agency, or should internal use of records be regulated as well?

INITIAL POLICY DECISIONS: Once it is determined which agencies and records should be covered, the policy approach of the legislation must be examined. Should the legislation prohibit anything not expressly authorized therein? Should it set goals to be achieved, leaving the implementation to others? Should it prohibit only known abuses, leaving all other decisions to the agency? Or what combinations of these approaches are feasible, based upon the nature of the information, the problems perceived, or the agencies covered?

ADMINISTRATION AND ENFORCEMENT: The possible courses of action in this area are many and may be used in a variety of combinations. Major possibilities are listed here but the list is not exhaustive.

Centralized control agency. A single agency could be created with the power both to administer and to enforce the provisions of any bill. It would issue the binding regulations and interpretations, order agencies to make changes and adjudicate individual complaints.

Agency control. A bill could vest all implementation authority in a criminal justice agency with respect to its own systems, relying on civil or criminal enforcement in individual cases to ensure compliance with the provisions of the bill.

Monitoring system: A bill could give implementation authority to each agency in the first instance but establish some form of general oversight in an independent body. The powers that might be given to a monitoring agency range from the review of regulations before they are issued to reporting on compliance on an on-going basis.

Private enforcement. There is a question whether a bill that regulates criminal justice information should permit private enforcement through individual law suits—either injunctive actions, damage actions, or both. If such enforcement is authorized, a number of subsidiary issues are raised. Should it be injunctive only, damage suit only, or both? Should suit be available against agencies, against individuals, or both? Should only actual damages be recoverable or should punitive or exemplary damages be authorized in certain cases? What defenses are available? May costs and attorneys fees be recovered and, if so, should monetary limits be set? Should there be liquidated damages—specified amounts—for injuries whose cost is difficullt to calculate?

Criminal enforcement. The basic issue is whether noncompliance with the provisions of a criminal justice information bill is a proper subject for criminal penalties. If so, should the penalties be limited to egregious cases or applied to all violations? Is it proper to impose penalties on recipients and users of information outside the criminal justice system as well as on the disseminators who are within the system? May the press be subjected to criminal penalties for using certain information? What defenses should be available with respect to charges of criminal violations of a law governing the handling of criminal justice information?

PRESS ACCESS: One of the most troublesome aspects of any criminal justice information bill is its impact on the press. If certain information is to be protected from public disclosure, then it must not be available to the press. On the other hand, the press can serve as a safeguard against abuses in the system but only if it has access to information. If certain information, such as rap sheets, consists entirely of notations of matters that were originally public information, can the compilation of the information properly be denied to the press? Is a distinction feasible between current information available to the press and past history that is not available?

INDIVIDUAL ACCESS TO RECORDS: It seems to be generally agreed that an individual's access to his own records is an important aspect of any privacy legislation. With respect to criminal justice records, however, unique problems arise.

Rap Sheet Data. Should an individual have access to his own rap sheet? Should access be permitted wherever the information may be located or only at certain repositories? Who has the responsibility to correct data? What procedures should be followed in providing correction? Is it preferable to give an individual a copy of his rap sheet or to let him inspect it only at some official location? Should data be available only to the individual or also to others at his request and with his consent?

Correctional records. Should an individual have full access to correctional records or may they be restricted? How should records of other agencies in a correctional file—presentence reports, psychiatrist's reports, etc.—be handled? Rather than blanket access, are case-by-case determinations possible?

Intelligence and investigative records. Can access be permitted without jeopardizing law enforcement interests? Is the granting of access consistent with the rules of discovery in criminal proceedings? If access to active files is denied, can access to closed files be authorized after a limited period? If so, what period is reasonable? Can proper distinctions be made with respect to access to investigative files vs. intelligence files?

Audit trails. If audit trails are required as to dissemination of any of these categories of information, should an individual have access to the audit trail? Can distinctions properly be made among the various types of information regarding access to audit trails? Is there a proper distinction between records of criminal justice access and records of noncriminal justice access in connection with permitting individual access to audit trails?

SEALING AND EXPUNGEMENT: Among the more controversial proposals with respect to criminal justice records is the suggestion that some or all of these records should be sealed or expunged after a period of time. With respect to each category of records the initial decision is whether there should be any sealing or expungement at all. If there is, which is the preferable form? Expungement, if effectively carried out, admits of no exceptions—the record ceases to exist. Sealing on the other hand may permit exceptions—the seal on any given record can be broken for specified reasons. Whichever form is considered—expungement or sealing—the questions remain as to which records are subject to it, and after what period of time.

AUTOMATED VS. MANUAL SYSTEMS: Whether valid or not, there appears to be more public concern about automated criminal justice information systems than about manual ones. The question arises whether greater restrictions should be placed on the use of automated systems than on manual systems and, if so, what restrictions. Among the restrictions that have been suggested are total prohibitions on patrol car or other mobile terminals, requirements of formal agreements governing access to automated systems, and requirements that automated centralized systems operate on a "pointer system" * rather than store information directly.

NONCRIMINAL JUSTICE ACCESS: While it is generally conceded that noncriminal justice access to criminal justice information should be regulated, the form of regulation raises a number of issues. Should only conviction information be available or may other rap sheet information be provided? Under what circumstances, if any, should investigative or intelligence information be available for non-criminal justice purposes? Is it necessary to make some correctional information available for noncriminal justice purposes in order to secure rehabilitation services? What should determine noncriminal justice access to criminal justice information: legislation dealing specifically with criminal justice information, other legislation, executive orders, or agency regulations? Can record-keeping and other restrictions, such as nonretention, insure against abuse of the information by noncriminal justice agencies? Here again, the issues are almost endless.

ARREST RECORDS: A serious problem concerns access to arrest information, i.e., information that notes only an arrest and does not indicate any disposition of charges. One solution is to prohibit dissemination of an arrest record outside the arresting agency, thus denying the information to noncriminal justice agencies and to other criminal justice agencies as well. A variation is to

* "Pointer" is frequently used to characterize an index which merely indicates what agency, if any, has a record on an individual, but the pointer system does not centrally store the record.

permit access to current arrest information but to bar access to information concerning arrests for which no disposition is indicated within a reasonable specified time. Another approach is narrowly to define the circumstances in which criminal justice and noncriminal justice agencies may have access to arrest information. Sealing and expungement discussed above, are particularly relevant to some of these considerations.

It is suggested that the issues outlined here will provide a starting point for any discussions of criminal justice information appropriate for enactment or amendment at the state level.

ILLUSTRATIVE LEGISLATION

The Seminar materials pertaining to criminal justice information systems also included existing statutes from Alaska, Iowa and Massachusetts, and a Model State Act for Criminal Offender Record Information produced by Project Search, all of which are reprinted below:

ALASKA STATUTES

CHAPTER 62. CRIMINAL JUSTICE INFORMATION SYSTEMS SECURITY AND PRIVACY

Section
10. Regulations
20. Collection and storage
30. Access and use
40. Security, updating, and purging
50. Interstate systems for the exchange of criminal justice information
60. Civil and criminal remedies
70. Definitions

Effective date—Section 3, ch, 161, SLA 1972, provides: "This Act takes effect October 1, 1972."

Sec. 12.62.010. **Regulations.** (a) The Governor's Commission on the Administration of Justice established under AS 44.19.746—44.19.758 is authorized, after appropriate consultation with representatives of state and local law enforcement agencies participating in information systems covered by this chapter, to establish rules, regulations, and procedures considered necessary to facilitate and regulate the exchange of criminal justice information and to insure the security and privacy of criminal justice information systems. The notice and hearing requirements of the Administrative Procedure Act (AS 44.62), relating to the adoption of regulations, apply to regulations adopted under this chapter. (§ 1 ch 161 SLA 1972)

Sec. 12.62.020. **Collection and storage.** (a) The commission shall establish regulations concerning the specific classes of criminal justice information which may be collected and stored in criminal justice information systems.

(b) No information collected under the provisions of any of the following titles of the Alaska Statutes, except for information related to criminal offenses under those titles, may be collected or stored in criminal justice information systems:

(1) AS 02, except chs. 20, 30 and 35;
(2) AS 03—04;
(3) AS 05, except chs. 20, 25, 30 and 35;
(4) AS 06—10;
(5) AS 13—15;
(6) AS 17;
(7) AS 18, except AS 18.60.120—18.60.175 and ch. 65;
(8) AS 19—27;
(9) AS 29—32;
(10) AS 34—46; and
(11) AS 47, except ch. 10.

(§ 1 ch 161 SLA 1972)

Sec. 12.62.030. **Access and use.** (a) Except as provided in (b) and (c) of this section, access to specified classes of criminal justice information in criminal justice information systems is available only to individual law enforcement agencies according to the specific needs of the agency under regulations established by the commission under § 10 of this chapter. Criminal justice information may be used only for law enforcement purposes or for those additional lawful purposes necessary to the proper enforcement or administration of other provisions of law as the commission may prescribe by regulations established under § 10 of this chapter. No criminal justice information may be disseminated to an agency before the commission determines the agency's eligibility to receive that information.

(b) Criminal justice information may be made available to qualified persons for research related to law enforcement under regulations established by the commission. These regulations must include procedures to assure the security of information and the privacy of individuals about whom information is released.

(c) A person shall have the right to inspect criminal justice information which refers to him. If a person believes the information to be inaccurate, incomplete or misleading, he may request the criminal justice agency having custody or control of the records to purge, modify or supplement them. If the agency declines to do so, or if the person believes the agency's decision to be otherwise unsatisfactory, the person may in writing request review by the commission within 60 days of the decision of the agency. The commission, its representative or agent shall, in a case in which it finds a basis for complaint, conduct a hearing at which the person may appear with counsel, present evidence, and examine and cross-examine witnesses. Written findings and conclusions shall be issued. If the record in question is found to be inaccurate, incomplete or misleading, the commission shall order it to be appropriately purged, modified or supplemented by an explanatory notation. An agency or person in the state with custody, possession or control of the record shall promptly have every copy of the record altered in accordance with the commission's order. Notification of a deletion, amendment and supplementary notation shall be promptly disseminated by the commission to persons or agencies to which records in question have been communicated, as well as to the person whose records have been altered.

(d) An agency holding or receiving criminal justice information shall maintain, for a period determined by the

commission to be appropriate, a listing of the agencies to which it has released or communicated the information. These listings shall be reviewed from time to time by the commission or staff members of the commission to determine whether the provisions of this chapter or any applicable regulations have been violated.

(e) Reasonable hours and places of inspection, and any additional restrictions, including fingerprintings, that are reasonably necessary both to assure the record's security and to verify the identities of those who seek to inspect them may be prescribed by published rules. Fingerprints taken under this subsection may not be transferred to another agency or used for any other purpose.

(f) A person or agency aggrieved by an order or decision of the commission under (c) of this section may appeal the order or decision to the superior court. The court shall in each case conduct a de novo hearing and may order the relief it determines to be necessary. If a person about whom information is maintained by an agency challenges that information in an action under this subsection as being inaccurate, incomplete or misleading, the burden is on the agency to prove that the information is not inaccurate, incomplete or misleading. (§ 1 ch 161 SLA 1972)

Sec. 12.62.040. **Security, updating, and purging.** (a) Criminal justice information systems shall

(1) be dedicated to law enforcement purposes and be under the management and control of law enforcement agencies unless exempted under regulations prescribed under § 10 of this chapter;

(2) include operating procedures approved by the commission which are reasonably designed to assure the security of the information contained in the system from unauthorized disclosure, and reasonably designed to assure that criminal offender record information in the system is regularly and accurately revised to include subsequently furnished information;

(3) include operating procedures approved by the commission which are designed to assure that information concerning an individual shall be removed from the records, based on considerations of age, nature of record, and reasonable interval following the last entry of information indicating that the individual is still under the jurisdiction of a law enforcement agency.

(b) Notwithstanding any provision of this section, any criminal justice information relating to minors which is maintained as part of a criminal justice information system must be afforded at least the same protection and is subject to the same procedural safeguards for the benefit of the individual with respect to whom the information is maintained, in matters relating to access, use and security as it would be under AS 47.10.090. (§ 1 ch 161 SLA 1972)

Sec. 12.62.050. **Interstate systems for the exchange of criminal justice information.** (a) The commission shall regulate the participation by all state and local criminal justice agencies in an interstate system for the exchange of criminal justice information, and shall be responsible to assure the consistency of the participation with the provisions and purposes of this chapter. The commission may not compel any criminal justice agency to participate in an interstate system.

(b) Direct access to an interstate system for the exchange of criminal justice information shall be limited to those criminal justice agencies that are expressly designated for that purpose by the commission. When the system employs telecommunications access terminals, the commission shall limit the number and placement of the terminals to those for which adequate security measures may be taken and as to which commission may impose appropriate supervisory regulations. (§ 1 ch 161 SLA 1972)

Sec. 12.62.060. **Civil and criminal remedies.** (a) A person with respect to whom criminal justice information has been wilfully maintained, disseminated, or used in violation of this chapter has a civil cause of action against the person responsible for the violation and shall be entitled to recover actual damages and reasonable attorney fees and other reasonable litigation costs.

(b) A person who wilfully disseminates or uses criminal justice information knowing such dissemination or use to be in violation of this chapter, upon conviction, is punishable by a fine of not more than $1,000 or by imprisonment for not more than one year, or by both.

(c) A good faith reliance upon the provisions of this chapter or of applicable law governing maintenance, dissemination, or use of criminal justice information, or upon rules, regulations, or procedures prescribed under this chapter is a complete defense to a civil or criminal action brought under this chapter. (§ 1 ch 161 SLA 1972)

Sec. 12.62.070. **Definitions.** In this chapter

(1) "criminal justice information system" means a system, including the equipment, facilities, procedures, agreements, and organizations related to the system funded in whole or in part by the Law Enforcement Assistance Administration, for the collection, processing, or dissemination of criminal justice information;

(2) "criminal justice information" means information concerning an individual in a criminal justice information system and indexed under the individual's name, or retrievable by reference to the individual by name or otherwise and which is collected or stored in a criminal justice information system;

(3) "commission" means the Governor's Commission on the Administration of Justice established under AS 44.19.746—44.19.758;

(4) "Interstate systems" means agreements, arrangements and systems for the interstate transmission and exchange of criminal justice information, but does not include record keeping systems in the state maintained or controlled by a state or local agency, or group of agencies, even if the agency receives information through, or otherwise participates in, systems for the interstate exchange of criminal justice information;

(5) "law enforcement" means any activity relating to crime prevention, control or reduction or the enforcement of the criminal prevention, control or reduction or the enforcement of the criminal law, including, but not limited to, police efforts to prevent, control or reduce crime or to apprehend criminals, activities of criminal prosecution, courts, public defender, corrections, probation or parole authorities;

(6) "law enforcement agency" means a public agency which performs as one of its principal functions activities pertaining to law enforcement. (§ 1 ch 161 SLA 1972)

IOWA

CHAPTER 294
CRIMINAL HISTORY DATA
S. F. 115

AN ACT relating to disclosure of criminal history and intelligence data and providing penalties.

Be It Enacted by the General Assembly of the State of Iowa:

SECTION 1. NEW SECTION. **Definitions of words and phrases.** As used in this Act, unless the context otherwise requires:

1. "Department" means the department of public safety.

2. "Bureau" means the department of public safety, division of criminal investigation and bureau of identification.

3. "Criminal history data" means any or all of the following information maintained by the department or bureau in a manual or automated data storage system and individually identified:

a. Arrest data.

b. Conviction data.

c. Disposition data.

d. Correctional data.

4. "Arrest data" means information pertaining to an arrest for a public offense and includes the charge, date, time, and place. Arrest data includes arrest warrants for all public offenses outstanding and not served and includes the filing of charges, by preliminary information when filed by a peace officer or law enforcement officer or indictment, the date and place of alleged commission and county of jurisdiction.

5. "Conviction data" means information that a person was convicted of or entered a plea of guilty to a public offense and includes the date and location of commission and place and court of conviction.

6. "Disposition data" means information pertaining to a recorded court proceeding subsequent and incidental to a public offense arrest and includes dismissal of the charge, suspension or deferral of sentence.

7. "Correctional data" means information pertaining to the status, location and activities of persons under the supervision of the county sheriff, the division of corrections of the department of social services, board of parole or any other state or local agency performing the same or similar function, but does not include investigative, sociological, psychological, economic or other subjective information maintained by the divsion of corrections of the department of social services or board of parole.

8. "Public offense" as used in subsections four (4), five (5), and six (6) of this section does not include nonindictable offenses under either chapter three hundred twenty-one (321) of the Code or local traffic ordinances.

9. "Individually identified" means criminal history data which relates to a specific person by one or more of the following means of identification:

a. Names and alias, if any.

b. Social security number.

c. Fingerprints.

d. Other index cross-referenced to paragraphs a, b, or c.

e. Other individually identifying characteristics.

10. "Criminal justice agency" means any agency or department of any level of government which performs as its principal function the apprehension, prosecution, adjudication, incarceration, or rehabilitation of criminal offenders.

11. "Intelligence data" means information collected where there are reasonable grounds to suspect involvement or participation in criminal activity by any person.

12. "Surveillance data" means information on individuals, partaining to participation in organizations, groups, meetings or assemblies, where there are no reasonable grounds to suspect involvement or participation in criminal activity by any person.

SEC. 2. NEW SECTION. **Dissemination of criminal history data.** The department and bureau may provide copies or communicate information from criminal history data only to criminal justice agencies, or such other public agencies as are authorized by the confidential records council. The bureau shall maintain a list showing the individual or agency to whom the data is disseminated and the date of dissemination.

Authorized agencies and criminal justice agencies shall request and may receive criminal history data only when:

1. The data is for official purposes in connection with prescribed duties, and

2. The request for data is based upon name, fingerprints, or other individual identifying characteristics.

The provisions of this section and section three (3) of this Act which relate to the requiring of an individually * identified request prior to the dissemination or redissemina-

* According to enrolled Act.

tion of criminal history data shall not apply to the furnishing of criminal history data to the federal bureau of investigation or to the dissemination or redissemination of information that an arrest warrant has been or will be issued, and other relevant information including but not limited to, the offense and the date and place of alleged commission, individually identifying characteristics of the person to be arrested, and the court or jurisdiction issuing the warrant.

SEC. 3. NEW SECTION. **Redissemination.** A peace officer, criminal justice agency, or state or federal regulatory agency shall not redisseminate criminal history data, within or without the agency, received from the department or bureau, unless:

1. The data is for official purposes in connection with prescribed duties of a criminal justice agency, and

2. The agency maintains a list of the persons receiving the data and the date and purpose of the dissemination, and

3. The request for data is based upon name, fingerprints, or other individual identification characteristics.

A peace officer, criminal justice agency, or state or federal regulatory agency shall not redisseminate intelligence data, within or without the agency, received from the department or bureau or from any other source, except as provided in subsections one (1) and two (2) of this section.

SEC. 4. NEW SECTION. **Statistics.** The department, bureau, or a criminal justice agency may compile and disseminate criminal history data in the form of statistical reports derived from such information or as the basis of further study provided individual identities are not ascertainable.

The bureau may with the approval of the commissioner of public safety disseminate criminal history data to persons conducting bona fide research, provided the data is not individually identified.

SEC. 5. NEW SECTION. **Right of notice, access and challenge.** Any person or his attorney with written authorization and fingerprint identification shall have the right to examine criminal history data filed with the bureau that refers to the person. The bureau may prescribe reasonable hours and places of examination.

Any person who files with the bureau a written statement to the effect that a statement contained in the criminal history data that refers to him is nonfactual, or information not authorized by law to be kept, and requests a correction or elimination of that information that refers to him shall be notified within twenty days by the bureau, in writing, of the bureau's decision or order regarding the correction or elimination. The bureau's decision or order or failure to allow examination may be appealed to the district court of Polk county by the person requesting said examination, correction or elimination. Immediately upon such appeal the court shall order the bureau to file with the court a certified copy of the criminal history data and in no other situation shall the bureau furnish an individual or his attorney with a certified copy, except as provided by this Act.

Upon the request of the appellant, the record and evidence in such cases shall be closed to all but the court and its officers, and access thereto shall be refused unless otherwise ordered by the court. The clerk shall maintain a separate docket for such actions. No person, other than the appellant shall permit a copy of any of the testimony or pleadings or the substance thereof to be made available to any person other than a party to the action or his attorney. Violation of the provisions of this section shall be a public offense, punishable under section seven (7) of this Act.

Whenever the bureau corrects or eliminates data as requested or as ordered by the court, the bureau shall advise all agencies or individuals who have received the incorrect information to correct their files. Upon application to the district court and service of notice on the commissioner of public safety, any individual may request and obtain a list of all persons and agencies who received criminal history data referring to him, unless good cause be shown why the individual should not receive said list.

SEC. 6. NEW SECTION. **Civil remedy.** Any person may institute a civil action for damages under chapters twenty-five A (25A) or six hundred thirteen A (613A) of the Code or to restrain the dissemination of his criminal history data or intelligence data in violation of this Act, and any person, agency or governmental body proven to have disseminated or to have requested and received criminal history data or intelligence data in violation of this Act shall be liable for actual damages and exemplary damages for each violation and shall be liable for court costs, expenses, and reasonable attorneys' fees incurred by the party bringing the action. In no case shall the award for damages be less than one hundred dollars.

SEC. 7. NEW SECTION. **Criminal penalties.**

1. Any person who willfully requests, obtains, or seeks to obtain criminal history data under false pretenses, or who willfully communicates or seeks to communicate criminal history data to any agency or person except in accordance with this Act, or any person connected with any research program authorized pursuant to this Act who willfully falsifies criminal history data or any records relating thereto, shall, upon conviction, for each such offense be punished by a fine of not more than one thousand dollars or by imprisonment in the state penitentiary for not more than two years, or by both fine and imprisonment. Any person who knowingly, but without criminal purposes, communicates or seeks to communicate criminal history data except in accordance with this Act shall for each such offense be fined not more than one hundred dollars or be imprisoned not more than ten days.

ILLUSTRATIVE
LEGISLATION

2. Any person who willfully requests, obtains, or seeks to obtain intelligence data under false pretenses, or who willfully communicates or seeks to communicate intelligence data to any agency or person except in accordance with this Act, shall for each such offense be punished by a fine of not more than five thousand dollars or by imprisonment in the state penitentiary for not more than three years, or by both fine and imprisonment. Any person who knowingly, but without criminal purposes, communicates or seeks to communicate intelligence data except in accordance with this Act shall for each such offense be fined not more than five hundred dollars or be imprisoned not more than six months, or both.

3. If the person convicted under this section is a peace officer, the conviction shall be grounds for discharge or suspension from duty without pay and if the person convicted is a public official or public employee, the conviction shall be grounds for removal from office.

4. Any reasonable grounds for belief that a public employee has violated any provision of this Act shall be grounds for immediate removal from all access to criminal history data and intelligence data.

SEC. 8. NEW SECTION. **Intelligence data.** Intelligence data contained in the files of the department of pubic safety or a criminal justice agency shall not be placed within a computer data storage system.

Intelligence data in the files of the department may be disseminated only to a peace officer, criminal justice agency, or state or federal regulatory agency, and only if the department is satisfied that the need to know and the intended use are reasonable. Whenever intelligence data relating to a defendant for the purpose of sentencing has been provided a court, the court shall inform the defendant or his attorney that it is in possession of such data and shall, upon request of the defendant or his attorney, permit examination of such data.

If the defendant disputes the accuracy of the intelligence data, he shall do so by filing an affidavit stating the substance of the disputed data and wherein it is inaccurate. If the court finds reasonable doubt as to the accuracy of such information, it may require a hearing and the examination of witnesses relating thereto on or before the time set for sentencing.

SEC. 9. NEW SECTION. No surveillance data shall be placed in files or manual or automated data storage systems by the department or bureau or by any peace officer or criminal justice agency. Violation of the provisions of this section shall be a public offense punishable under section seven (7) of this Act.

SEC. 10. NEW SECTION. **Rules.** The department shall adopt rules and regulations designed to assure the security and confidentiality of all criminal history data and intelligence data systems.

SEC. 11. NEW SECTION. **Education program.** The department shall require an educational program for its employees and the employees of criminal justice agencies on the proper use and control of criminal history data and intelligence data.

SEC. 12. NEW SECTION. **Data processing.** Nothing in this Act shall preclude the use of the equipment and hardware of the data processing service center provided for in section nineteen B point three (19B.3), subsection five (5), of the Code for the storage and retrieval of criminal history data. Files shall be stored on the computer in such a manner as the files cannot be modified, destroyed, accessed, changed or overlayed * in any fashion by noncriminal justice agency terminals or personnel. That portion of any computer, electronic switch or manual terminal having access to criminal history data stored in the state computer must be under the management control of a criminal justice agency.

SEC. 13. NEW SECTION. **Review.** The department shall initiate periodic review procedures designed to determine compliance with the provisions of this Act within the department and by criminal justice agencies and to determine that data furnished to them is factual and accurate.

SEC. 14. NEW SECTION. **System for the exchange of criminal history data.** The department shall regulate the participation by all state and local agencies in any system for the exchange of criminal history data, and shall be responsible for assuring the consistency of such participation with terms and purposes of this Act.

Direct access to such systems shall be limited to such criminal justice agencies as are expessly designated for that purpose by the department. The department shall, with respect to telecommunications terminals employed in the discrimination of criminal history data, insure that security is provided over an entire terminal or that portion actually authorized access to criminal history data.

SEC. 15. NEW SECTION. **Reports to department.** When it comes to the attention of a sheriff, police department, or other law enforcement agency that a public offense has been committed in its jurisdiction, it shall be the duty of the law enforcement agency to report information concerning such crimes to the bureau on a form to be furnished by the bureau not more than thirty-five days from the time the crime first comes to the attention of such law enforcement agency. These reports shall be used to generate crime statistics. The bureau shall submit statistics to the governor, legislature and crime commission on a quarterly and yearly basis.

When a sheriff, police department or other law enforcement agency makes an arrest which is reported to the bureau, the arresting law enforcement agency and any other law enforcement agency which obtains custody of the arrested person shall furnish a disposition report to the

* According to enrolled Act.

bureau whenever the arrested person is transferred to the custody of another law enforcement agency or is released without having a complaint or information filed with any court.

Whenever a criminal complaint or information is filed in any court, the clerk shall furnish a disposition report of such case.

The disposition report, whether by a law enforcement agency or court, shall be sent to the bureau within thirty days after disposition on a form provided by the bureau.

SEC. 16. NEW SECTION. **Review and removal.** At least every year the bureau shall review and determine current status of all Iowa arrests reported after the effective date of this Act which are at least one year old with no disposition data. Any Iowa arrest recorded within a computer data storage system which has no disposition data after five years shall be removed unless there is an outstanding arrest warrant or detainer on such charge.

SEC. 17. NEW SECTION. **Exclusion.** Criminal history data in a computer data storage system does not include:

1. Arrest or disposition data after the person has been acquitted or the charges dismissed.

SEC. 18. NEW SECTION. **Public records.** Nothing in this Act shall prohibit the public from examining and copying the public records of any public body or agency as authorized by chapter sixty-eight A (68A) of the Code.

Criminal history data and intelligence data in the possession of the department or bureau, or disseminated by the department or bureau, are not public records within the provisions of chapter sixty-eight A (68A) of the Code.

SEC. 19. NEW SECTION. There is hereby created a confidential records council consisting of nine regular members. Two members shall be appointed from the house of representatives by the speaker of the house, no more than one of whom shall be from the same party. Two members shall be appointed from the senate by the lieutenant governor, no more than one of whom shall be from the same party. The other members of the council shall be: a judge of the district court appointed by the chief justice of the supreme court, one local law enforcement official, appointed by the governor; the commissioner of public safety or his designee; and two private citizens not connected with law enforcement, appointed by the governor. The council shall select its own chairman. The members shall serve at the pleasure of those by whom their appointments are made.

The council shall meet at least annually and at any other time upon the call of the governor, the chairman of the council, or any three of its members. Each council member shall be entitled to reimbursement for actual and necessary expenses incurred in the performance of official duties from funds appropriated to the department of public safety.

The council shall have the following responsibilities and duties:

1. Shall periodically monitor the operation of governmental information systems which deal with the collection, storage, use and dissamination of criminal history or intelligence data.

2. Shall review the implementation and effectiveness of legislation and administrative rules and regulations concerning such systems.

3. May recommend changes in said rules and regulations and legislation to the legislature and the appropriate administrative officials.

4. May require such reports from state agencies as may be necessary to perform its duties.

5. May receive and review complaints from the public concerning the operation of such systems.

6. May conduct such inquiries and investigations as it finds appropriate to achieve the purposes of this Act. Each criminal justice agency in this state and each state and local agency otherwise authorized access to criminal history data is authorized and directed to furnish to the council, upon its request, such statistical data, reports, and other information in its possession as the council deems necessary to carry out its functions under this Act. However, the council and its members, in such capacity, shall not have access to criminal history data or intelligence data unless it is data from which individual identities are not ascertainable or data which has been marked so that individual identities are not ascertainable. However, the council may examine data from which the identity of an individual is ascertainable if requested in writing by that individual or his attorney with written authorization and fingerprint identification.

7. Shall annually approve rules and regulations adopted in accordance with section ten (10) of this Act and rules and regulations to assure the accuracy, completeness and proper purging of criminal history data.

8. Shall approve all agreements, arrangements and systems for the interstate transmission and exchange of criminal history data.

SEC. 20. NEW SECTION. The provisions of sections two (2) and three (3) of this Act shall not apply to the certifying of an individual's operating record pursuant to section three hundred twenty-one A point three (321A.3) of the Code.

Approved July 21, 1973.*

COMMONWEALTH OF MASSACHUSETTS

G.L. c. 6, s. 167-178, added by St. 1972, c. 805 including amendment in St. 1973, St. 961

* This Act was passed by the G. A. before July 1, 1973.

CRIMINAL OFFENDER RECORD INFORMATION SYSTEM
[NEW]

§ 167. Definitions

The following words shall, whenever used in this section or in sections one hundred and sixty-eight to one hundred seventy-eight, inclusive, have the following meanings unless the context otherwise requires: "Criminal justice agencies", those agencies at all levels of government which perform as their principal function, activities relating to *(a)* crime prevention, including research or the sponsorship of research; *(b)* the apprehension, prosecution, adjudication, incarceration, or rehabilitation of criminal offenders; or *(c)* the collection, storage, dissemination or usage of criminal offender record information.

"Criminal offender record information", records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation and release. Such information shall be restricted to that recorded as the result of the initiation of criminal proceedings or of any consequent proceedings related thereto. It shall not include intelligence, analytical and investigative reports and files, nor statistical records and reports in which individuals are not identified and from which their identities are not ascertainable.

"Interstate systems", all agreements, arrangements and systems for the interstate transmission and exchange of criminal offender record information. Such systems shall not include recordkeeping systems in the commonwealth maintained or controlled by any state or local agency, or group of such agencies, even if such agencies receive or have received information through, or otherwise participated or have participated in, systems for the interstate exchange of criminal record information.

"Purge", remove from the criminal offender record information system such that there is no trace of information removed and no indication that said information was removed.

Added by St.1972, c. 805, § 1.

1972 Enactment. St.1972, c. 805, § 1, adding this section and sections 168 to 178 of this chapter, was approved July 19, 1972. Section 9 provided: "This act shall take effect conformably to law, except that any agency, department, institution, or individual which is authorized by statute to receive criminal offender record information or which receives the same at the discretion of the commissioner of probation, on the effective date of this act, shall continue to receive the same, notwithstanding any provision of this act to the contrary, until January first, nineteen hundred and seventy-three."

Cross References

Correctional institutions.
  Identification of prisoners, see c. 127, § 23.
  Fugitives from justice, descriptions, see c. 127, § 25.
Department of public safety, criminal information bureau, see c. 22, § 3A.
Fingerprinting and photographing.
  Cities and towns, persons arrested during riots, etc., see c. 41, § 98.
  Persons charged with a felony, see c. 263, § 1A.
Use of systems operated by the board authorized.
  Commissioner of probation, see c. 276, § 100.
  Correctional institutions, see c. 127, §§ 2, 28, 29.
Department of public safety, see c. 147, § 4A.
State police, criminal information bureau, see c. 147, § 4C.

§ 168. Criminal history systems board; establishment; members; chairman; terms; meetings; expenses; regulations; powers and duties; director of teleprocessing and other employees; report

There shall be a criminal history systems board, hereinafter called the board, consisting of the following persons: the attorney general, the chairman of the Massachusetts defenders committee, the chairman of the parole board, the chief justice of the district courts, the chief justice of the superior court, the chief justice of the supreme judicial court, the commissioner of the department of correction, the commissioner of the department of public safety, the commissioner of the department of youth services, the commissioner of probation, the executive director of the governor's public safety committee, and the police commissioner of the city of Boston, or their designees, all of whom shall serve ex officio, and three other persons to be appointed by the governor for a term of three years one of whom shall represent the Massachusetts district attorneys association, one of whom shall represent the Massacusetts chiefs of police association, and one of whom shall represent the county commissioners and sheriffs association. Upon the expiration of the term of any appointive member his successor shall be appointed in a like manner for a term of three years.

The governor shall designate annually the chairman of the board from among its members. No chairman may be appointed to serve more than two consecutive terms. The chairman shall hold regular meetings, one of which shall be an annual meeting and shall notify all board members of the time and place of all meetings. Special meetings may be called at any time by a majority of the board members and shall be called by the chairman upon written application of eight or more members. Members of the board shall receive no compensation, but shall receive their expenses actually and necessarily incurred in the discharge of their duties.

The board, after receiving the advice and recommendations of its advisory committee, shall, with the approval of two-thirds of the board members or their designees present and voting, promulgate regulations regarding the collection, storage, dissemination and usage of criminal offender record information.

The board shall provide for and exercise control over the installation, operation and maintenance of data processing and data communication systems, hereinafter

called the criminal offender record information system. Said system shall be designed to insure the prompt collection, exchange, dissemination and distribution of such criminal offender record information as may be necessary for the efficient administration and operation of criminal justice agencies, and to connect such systems directly or indirectly with similar systems in this or other states. The board shall appoint, subject to section one hundred and sixty-nine, and fix the salary of a director of teleprocessing who shall not be subject to the provisions of chapter thirty-one or of section nine A of chapter thirty. The board may appoint such other employees, including experts and consultants, as it deems necessary to carry out its responsibilities, none of whom shall be subject to the provisions of chapter thirty-one or of section nine A of chapter thirty.

The board shall make an annual report to the governor and file a copy thereof with the state secretary, the clerk of the house of representatives and the clerk of the senate.

The board is authorized to enter into contracts and agreements with, and accept gifts, grants, contributions, and bequests of funds from, any department, agency, or subdivision of federal, state, county, or municipal government and any individual, foundation, corporation, association, or public authority for the purpose of providing or receiving services, facilities, or staff assistance in connection with its work. Such funds shall be deposited with the state treasurer and may be expended by the board in accordance with the conditions of the gift, grant, contribution, or bequest, without specific appropriation.

Policies, rules and regulations shall not be adopted by the board until a hearing has been held in the manner provided by section two of chapter thirty A.

Added by St.1972, c. 805 § 1. Amended by St.1973, c. 961, § 1.

1973 Amendment. St.1973, c. 961, § 1, approved Oct. 29, 1973, added the last paragraph.

§ 169. Criminal history system advisory committee; establishment; members; vote; chairman; executive secretary, et al.; meetings; powers, duties and functions; participation in interstate system for exchange of record information; reports

There shall be a criminal history system advisory committee of the board, hereinafter called the advisory committee, consisting of the following persons and their designees: the commissioner of the Boston police department, the attorney general, the commissioner of correction, the commissioner of public safety, the commissioner of youth services, the director of teleprocessing of the criminal offender record system, the executive director of the governor's public safety committee, the president of the Massachusetts district attorneys association, the commissioner of probation, the chairman of the parole board, and the chief justices of the district and superior courts. Each agency represented shall be limited to one vote regardless of the number of designees present at the time any votes are taken.

The advisory committee shall elect its own chairman from its membership to serve a term of one year. No chairman may be elected to serve more than two consecutive terms. The advisory committee may appoint an executive secretary, legal counsel and such other employees as it may from time to time deem appropriate to serve, provided, however, that such employees shall not be subject to chapter thirty-one or section nine A of chapter thirty.

The chairman shall hold regular meetings, one of which shall be an annual meeting and shall notify all advisory committee members of the time and place of all meetings. Special meetings shall be called at any time by a majority of the advisory committee members, and shall be called by the chairman upon written application of seven or more members.

The advisory committee shall recommend to the board regulations relating to the collection, storage, dissemination and use of criminal offender record information. The advisory committee shall ensure that communication is maintained among the several prime users. The advisory committee shall also recommend to the board the director of teleprocessing of the criminal offender record information system.

The advisory committee may coordinate its activities with those of any interstate systems for the exchange of criminal offender record information, may nominate one or more of its members to serve upon the council or committee of any such system and may participate when and as it deems appropriate in any such system's activities and programs.

The advisory committee may conduct such inquiries and investigations as it deems necessary and consistent with its authority. It may request any agency that maintains, receives, or that is eligible to maintain or receive criminal offender records to produce for inspection statistical data, reports and other information concerning the collection, storage, dissemination and usage of criminal offender record information. Each such agency is authorized and directed to provide such data, reports, and other information.

The advisory committee, shall report annually to the board concerning the collection, storage, dissemination and usage of criminal offender record information in the commonwealth. The board may require additional reports as it deems advisable.

Policies, rules and regulations shall not be adopted by the advisory committee until a hearing has been held in the manner provided by section two of chapter thirty A.

Added by St.1972, c. 805. § 1. Amended by St.1973, c. 961, § 2.

1973 Amendment. St.1973, c. 961, § 2, approved Oct. 29, 1973 added the last paragraph.

§ 170. Security and privacy council; establishment; members; chairman; terms; clerical assistance; meetings; duties and functions; expenses; reports; participation in interstate system for exchange of record information

There shall be a security and privacy council, hereinafter called the council, consisting of the chairman and one other member of the advisory committee, chosen by the advisory committee, and seven other members to be appointed by the governor, to include representatives of the general public, state and local government, and one representative of the criminal justice community. Of the seven members initially appointed by the governor, two shall be appointed for a period of one year, two shall be appointed for a period of two years, two shall be appointed for a period of three years, one shall be appointed for a period of four years. Thereafter, each of the appointments shall be for a period of four years. Each member appointed by the governor shall serve until his successor is appointed and has qualified. The chairman of the council shall be elected by and from within the council to serve for a term of two years. The advisory committee shall provide such clerical and other assistance as the council may require. The council shall meet at the call of the governor, its chairman, or any three of its members and shall conduct a continuing study and review and to make recommendations concerning questions of individual privacy and system security in connection with the collection, storage, dissemination, and usage of criminal offender record information. Council members shall receive no compensation for their services on the council but shall receive their expenses necessarily incurred in the performance of official duties.

The council may conduct such inquiries and investigations as it deems necessary and consistent with its authority. The board, each criminal justice agency in the commonwealth, and each state and local agency having authorized access to criminal offender record information, is authorized and may furnish to the council, upon request made by its chairman, such statistical data, reports, and other information directly related to criminal offender record information as is necessary to carry out the council's functions.

The council shall make an annual report to the governor and file a copy thereof with the state secretary and the clerk of the house of representatives and the clerk of the senate. It may make such additional reports and recommendations as it deems appropriate to carry out its duties.

The council shall appoint one or more of its members to serve upon any similar council or committee connected with any interstate system for the exchange of criminal offender record information, and may participate as it deems appropriate in the activities of any such system.

Policies, rules and regulations shall not be adopted by the council until a hearing has been held in the manner provided by section two of chapter thirty A.

Added by St.1972, c. 805, § 1. Amended by St.1973, c. 961, § 3.

1973 Amendment. St.1973, c. 961, § 3, approved Oct. 29, 1973, added the last paragraph.

§ 171. Regulations generally; continuing educational program

The board shall promulgate regulations *(a)* creating a continuing program of data auditing and verification to assure the accuracy and completeness of criminal offender record information; *(b)* assuring the prompt and complete purging of criminal record information, insofar as such purging is required by any statute or administrative regulation, by the order of any court of competent jurisdiction, or to correct any errors shown to exist in such information; and *(c)* assuring the security of criminal offender record information from unauthorized disclosures at all levels of operation.

The board shall cause to be initiated for employees of all agencies that maintain, receive, or are eligible to maintain or receive criminal offender record information a continuing educational program in the proper use and control of such information.

Added by St.1972, c. 805, § 1.

§ 172. Dissemination of record information to authorized agencies and individuals; determination of eligibility for access; certification; listing; scope of inquiry; regulations; access limited; authorization

Criminal offender record information shall be disseminated, whether directly or through any intermediary, only to *(a)* criminal justice agencies and *(b)* such other individuals and agencies as are authorized access to such records by statute.

The board shall certify which agencies and individuals requesting access to criminal offender record information are authorized such access. The board shall, regarding such agency or individual, make a finding in writing of eligibility or non-eligibility for such access. No such information shall be disseminated to any agency or individual prior to the board's determination of eligibility or, in cases in which the board's decision is appealed, prior to the final judgment of a court of competent jurisdiction that the agency or individual is so eligible.

Each agency holding or receiving criminal offender record information shall maintain, for such period as is found by the board to be appropriate, a listing of the agencies or individuals to which it has released or com-

municated such information. Such listings, or reasonable samples thereof, may from time to time be reviewed by the board, advisory committee, or council to determine whether any statutory provisions or regulations have been violated.

Dissemination from any agency in this commonwealth of criminal offender record information shall, except for purposes of research programs approved under section one hundred and seventy-three, be permitted only if the inquiry is based upon name, fingerprints or other personal identifying characteristics. The board shall promulgate regulations to prevent dissemination of such information, except in the above situations, where inquiries are based upon categories of offense or data elements other than said characteristics.

Notwithstanding the provisions of this section, access to criminal offender record information on the basis of data elements other than personal identifying characteristics shall be permissible if the criminal justice agency seeking such access has first obtained authorization from the commissioner of probation, or in his absence, a deputy commissioner of probation. Such authorization may be given as a matter of discretion in cases in which it has been shown that such access is imperative for purposes of the criminal justice agency's investigational or other responsibilities and the information sought to be obtained is not reasonably available from any other source or through any other method.
Added by St.1972, c. 805, § 1.

§ 173. Regulations for program research; monitoring; access restricted

The board shall promulgate regulations to govern the use of criminal offender record information for purposes of program research. Such regulations shall require preservation of the anonymity of the individuals to whom such information relates, shall require the completion of nondisclosure agreements by all participants in such programs, and shall impose such additional requirements and conditions as the board finds to be necessary to assure the protection of privacy and security interests.

The board may monitor any such programs to assure their effectiveness. The board may, if it determines that a program's continuance threatens privacy or security interests, prohibit access on behalf of any such program to criminal offender record information.
Added by St.1972, c. 805, § 1.

§ 174. Interstate system for exchange of record information; supervision of participation by state and local agencies; access limited; telecommunications access terminals

The board shall supervise the participation by all state and local agencies in any interstate systems for the exchange of criminal offender record information, and shall be responsible to assure the consistency of such participation with the terms and purposes of sections one hundred and sixty-eight to section one hundred and seventy-eight, inclusive.

Direct access to any such system shall be limited to such criminal justice agencies as are expressly designated for that purpose by the board. Where any such system employs telecommunications access terminals, the board shall limit the number and placement of such terminals to those for which adequate security measures may be taken and as to which the board may impose appropriate supervisory regulations.
Added by St.1972, c. 805, § 1.

§ 175. Inspection of record information by individual concerned; corrections; procedure; restrictions

Each individual shall have the right to inspect, and if practicable, copy, criminal offender record information which refers to him. If an individual believes such information to be inaccurate or incomplete, he shall request the agency having custody or control of the records to purge, modify or supplement them. If the agency declines to so act, or if the individual believes the agency's decision to be otherwise unsatisfactory, the individual may in writing request review by the council. The council shall, in each case in which it finds prima facie basis for complaint, conduct a hearing at which the individual may appear with counsel, present evidence, and examine and cross-examine witnesses. Written findings shall be issued within sixty days of receipt by the council of the request for review. Failure to issue findings shall be deemed a decision of the council. If the record in question is found to be inaccurate, incomplete or misleading, the council shall recommend to the board that the record be appropriately purged, modified or supplemented by explanatory notation. Notification of the council's recommendation and subsequent orders by the board to delete, amend or supplement the records, shall be disseminated by the board to any individuals or agencies to which the records in question have been communicated, as well as to the individual whose records have been ordered so altered within ten days of receipt of the council's recommendation. Failure of the board to act shall be deemed a decision of the board.

Agencies at which criminal offender records are sought to be inspected shall prescribe reasonable hours and places of inspection, and shall impose such additional restrictions as may be approved by the board, including fingerprinting, as are reasonably necessary both to assure the record's security and to verify the identities of those who seek to inspect them.
Added by St.1972, c. 805, § 1.

§ 176. Appeal; de novo hearing; equitable relief

Any individual or agency aggrieved by any order or decision of the board or adverse recommendation of the council or failure of the council to issue findings may appeal such order, recommendation or decision to the superior court in the county in which he is resident or in which the board issued the order or decision from which the individual or agency appeals. The court shall in each such case conduct a de novo hearing, and may order such relief as it finds to be required by equity.
Added by St.1972, c. 805, § 1.

§ 177. Violations; civil liability

Any aggrieved person may institute a civil action in superior court for damages or to restrain any violation of sections one hundred and sixty-eight to one hundred and seventy-five, inclusive. If it is found in any such action that there has occurred a willful violation, the violator shall not be entitled to claim any privilege absolute or qualified, and he shall in addition to any liability for such actual damages as may be shown, be liable for exemplary damages of not less than one hundred and not more than one thousand dollars for each violation, together with costs and reasonable attorneys' fees and disbursements incurred by the person bringing the action.
Added by St.1972, c. 805, § 1.

§ 178. Violations; punishment

Any person who willfully requests, obtains or seeks to obtain criminal offender record information under false pretenses, or willfully communicates or seeks to communicate criminal offender record information to any agency or person except in accordance with the provisions of sections one hundred and sixty-eight to one hundred and seventy-five, inclusive, or any member, officer, employee or agency of the board, the advisory committee, the council or any participating agency, or any person connected with any authorized research program, who willfully falsifies criminal offender record information, or any records relating thereto, shall for each offense be fined not more than five thousand dollars, or imprisoned in a jail or house of correction for not more than one year, or both.
Added by St.1972, c. 805, § 1.

PROJECT SEARCH

A Model State Act For Criminal Offender Record Information*

1. Legislative Findings and Purpose.

The legislature finds and declares that a more effective administrative structure now is required to control the collection, storage, dissemination and usage of criminal offender record information. These improvements in the organization and control of criminal offender recordkeeping are imperative both to strengthen the administration of criminal justice and to assure appropriate protection of rights of individual privacy. The legislature further finds that vigorous protection of such rights of individual privacy is an indispensable element of a fair and effective system of criminal offender recordkeeping. The purposes of this Act are (1) to control and coordinate criminal offender recordkeeping within this State; (2) to encourage more efficient and uniform systems of criminal offender recordkeeping; (3) to assure periodic reporting to the Governor and legislature concerning such recordkeeping; and (4) to establish a more effective administrative structure for the protection of individual privacy in connection with such recordkeeping.

2. Definitions.

For purposes of this Act, (a) "criminal justice agencies" shall be understood to include only those public agencies at all levels of government which perform as their principal function activities (i) relating to crime prevention, including research or the sponsorship of research; (ii) relating to the apprehension, prosecution, adjudication, or rehabilitation of criminal offenders; or (iii) relating to the collection, storage, dissemination or usage of criminal offender record information.

(b) "criminal offender record information" shall be understood to include records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, rehabilitation and release. Such information shall be understood to be restricted to that recorded as the result of the initiation of criminal proceedings or of any consequent proceedings related thereto. It shall be understood not to include intelligence, analytical and investigative reports and files, nor statistical records and reports in which individuals are not identified and from which their identities are not ascertainable.

(c) "interstate systems" shall be understood to include all agreements, arrangements and systems for the interstate transmission and exchange of criminal offender record information. Such systems shall be understood not to include recordkeeping systems in the state maintained or controlled by any state or local agency, or group of such agencies, even if such agencies receive or have received information through, or otherwise participate or have participated in, systems for the interstate exchange of criminal offender record information.

* Reprinted from Project Search Technical Memorandum No. 3, May, 1971.

(d) "state" shall be understood to mean, unless otherwise expressly indicated, this state.

3. Relationship to Other Statutes.

(a) In the event of conflict, this Act shall to the extent of the conflict supersede, except as provided in subsection (b), all existing statutes which regulate, control or otherwise relate, directly or by implication, to the collection, storage, dissemination or usage of criminal offender records. So far as consistent with this Act, the [state administrative code shall govern the transactions and proceedings conducted pursuant to this Act].

(b) Not withstanding the provisions of the subsection (a), this Act shall not be understood to alter, amend or supersede the statutes and rules of law which govern the collection, storage, dissemination or usage of records concerning juvenile or youthful offenders.

4. Criminal Offender Records Control Committee.

(a) The Criminal Offender Records Control Committee (hereinafter the Committee) is established to regulate the collection, storage, dissemination and usage of criminal offender record information. The Committee shall be composed of persons representing the following state and local criminal justice agencies: [————————]. The Committee's Chairman shall be appointed by [the Governor] and shall serve at his pleasure. The Committee may appoint and fix the compensation of a staff director, a legal counsel and such other staff personnel as it may from time to time deem appropriate.

(b) The Committee may coordinate its activities with those of any interstate systems for the exchange of criminal offender record information, may nominate one or more of its members to serve upon the council or committee of any such system, and may participate when and as it deems appropriate in any such system's activities and programs.

(c) The Committee shall adopt such regulations as it finds appropriate to carry out its functions under this Act.

(d) The Committee may conduct such inquiries and investigations as it finds appropriate to carry out its functions under this Act. It may for this purpose request any agency that maintains, or has received, or that is eligible to maintain or receive criminal offender records to produce for inspection statistical data, reports and other information concerning the collection, storage, dissemination and usage of criminal offender record information. Each such agency is authorized and directed to provide such data, reports, and other information.

(e) The Committee shall report annually to the Governor and legislature concerning the collection, storage, dissemination and usage in this state of criminal offender record information. The Governor or legislature may require such additional reports as they deem desirable.

5. Security and Privacy Council.

(a) [The Governor] shall appoint a Security and Privacy Council (hereinafter the Council), consisting of a chairman and not more than eight members, to conduct a continuing study and review of questions of individual privacy and system security in connection with the collection, storage, dissemination and usage of criminal offender record information. In appointing the Council, [the Governor] shall seek such representatives of the general public, state and local government, and the criminal justice community as may be expected to express fairly and vigorously the various interests involved. The Council's Chairman and members shall serve at [the Governor's] pleasure. The Council may appoint and fix the compensation of a staff director, a legal counsel and such other staff personnel as it may from time to time deem appropriate. The Council shall meet at the call of the Governor, its Chairman, or any three of its members to carry out its responsibilities under Section II of this Act, to study the privacy and security implications of criminal offender records, or to formulate recommendations concerning their collection, storage, dissemination or usage. Each Council member shall be entitled to reimbursement for actual and necessary expenses incurred in the performance of official duties.

(b) The Council may conduct inquiries and investigations as it finds appropriate to achieve the purposes of this Act. The Committee, each criminal justice agency in this state, and each state and local agency otherwise authorized access to criminal offender record information is authorized and directed to furnish to the Council, upon request made by its Chairman, such statistical data, reports, and other information as the Council deems necessary to carry out its functions under this Act.

(c) The Council shall report annually to the Governor and legislature concerning both its responsibilities under Section 11 and other questions of privacy and security in connection with the collection, storage, dissemination and usage of criminal offender record information. It may make such additional reports and recommendations as it deems appropriate to carry out its functions under this Act.

(d) The Council may nominate one or more of its members to serve upon any similar council or committee connected with any interstate system for the exchange of criminal offender record information, and may participate when and as it deems appropriate in the activities of any such system.

6. Data Verification and Purging.

(a) The Committee shall adopt regulations creating a continuing program of data auditing and verification to assure the accuracy and completeness of criminal offender record information.

(b) The Committee shall adopt regulations to assure the prompt and complete purging of criminal record information, insofar as such purging is required.

(i) by any statute or valid administrative regulation of this state;

(ii) by the order of any court of competent jurisdiction in this state;

(iii) by the law of any other jurisdiction, where the data or records in question have originated in that jurisdiction;

(iv) to correct any errors shown to exist in such information;

(v) to achieve any of the purposes of this Act, to improve the efficiency of criminal offender recordkeeping, or otherwise to promote the fair and efficient administration of criminal justice.

7. System Security.

(a) The Committee shall adopt regulations to assure the security of criminal offender record information from unauthorized disclosures at all levels of operation in this state.

(b) The Committee shall cause to be initiated for employees of all agencies that maintain, receive, or are eligible to maintain or receive criminal offender record information a continuing educational program in the proper use and control of such information.

8. Access.

(a) Criminal offender record information shall be disseminated, whether directly or through any intermediary, only to (i) criminal justice agencies and (ii) such other individuals and agencies as are, or may subsequently be, authorized access to such records by statute. The Committee shall issue regulations to assure that such information shall be disseminated only in situations in which it is demonstrably required by the individual or agency for purposes of its statutory responsibilities.

(b) It shall be the Committee's responsibility to determine whether each agency requesting access to criminal offender record information is authorized such access under the terms of this Act. The Committee shall, as to each such agency, make a finding in writing of its eligibility or non-eligibility for such access. Except as provided in subsection (c) of this section, no such information shall be disseminated to any agency prior to the Committee's determination of its eligibility or, in cases in which the Committee's decision is appealed under Section 12 of this Act, prior to the final judgment of a court of competent jurisdiction that the agency is so eligible.

(c) For a period of [six months] following the adoption of this Act, or until such time as the Committee completes its determination of the eligibility or non-eligibility for access of a requesting agency, whichever first occurs, any such requesting agency that is receiving criminal offender record information at the time of this Act's passage shall be deemed to be eligible for such access.

(d) Each agency holding or receiving criminal offender record information shall maintain, for such period as is found by the Committee to be appropriate, a listing of the agencies to which it has released or communicated such information. Such listings, or reasonable samples thereof, may from time to time be reviewed by the Committee, Council, or any of their staff members to determine whether this Act or any applicable regulations have been violated.

(e) Dissemination from any agency in this state of criminal offender record information shall, except for purposes of programs of research approved under Section 9, and with the further exception of instances in which a warrant has been obtained in accordance with subsection (f) of this section, be permitted only if the inquiry is based upon name, fingerprints or other personal identifying characteristics. The Committee shall issue regulations to prevent dissemination of such information, except in the above situations, where inquiries are based upon categories of offense or data elements other than name, fingerprints or other personal identifying characteristics.

(f) Notwithstanding the provisions of subsection (e), access to criminal offender record information on the basis of data elements other than personal identifying characteristics shall be permissible if the criminal justice agency seeking such access has first obtained from a (magistrate, judge or justice) a class access warrant. Such warrants may be issued as a matter of discretion by a (magistrate, judge or justice of any court of this state) in cases in which probable cause has been shown that (i) such access is imperative for purposes of the criminal justice agency's investigational or other responsibilities, and (ii) the information sought to be obtained is not reasonably available from any other source or through any other method. A summary of each request for such a warrant, together with a statement of its disposition, shall within ninety days of disposition be furnished the Committee.

9. Research.

(a) The Committee shall issue regulations to govern the usage in this state of criminal offender record information for purposes of programs of research. Such regulations shall require preservation of the anonymity of the individuals to whom such information relates, shall require the completion of nondisclosure agreements by all participants in such programs, and shall impose such additional requirements and conditions as the Committee finds to be necessary to assure the protection of privacy and security interests.

(b) The Committee may monitor any such programs to assure satisfaction both of the requirements of this Act and of any applicable regulations. The Committee may, if

(d) "state" shall be understood to mean, unless otherwise expressly indicated, this state.

3. Relationship to Other Statutes.

(a) In the event of conflict, this Act shall to the extent of the conflict supersede, except as provided in subsection (b), all existing statutes which regulate, control or otherwise relate, directly or by implication, to the collection, storage, dissemination or usage of criminal offender records. So far as consistent with this Act, the [state administrative code shall govern the transactions and proceedings conducted pursuant to this Act].

(b) Not withstanding the provisions of the subsection (a), this Act shall not be understood to alter, amend or supersede the statutes and rules of law which govern the collection, storage, dissemination or usage of records concerning juvenile or youthful offenders.

4. Criminal Offender Records Control Committee.

(a) The Criminal Offender Records Control Committee (hereinafter the Committee) is established to regulate the collection, storage, dissemination and usage of criminal offender record information. The Committee shall be composed of persons representing the following state and local criminal justice agencies: [————————]. The Committee's Chairman shall be appointed by [the Governor] and shall serve at his pleasure. The Committee may appoint and fix the compensation of a staff director, a legal counsel and such other staff personnel as it may from time to time deem appropriate.

(b) The Committee may coordinate its activities with those of any interstate systems for the exchange of criminal offender record information, may nominate one or more of its members to serve upon the council or committee of any such system, and may participate when and as it deems appropriate in any such system's activities and programs.

(c) The Committee shall adopt such regulations as it finds appropriate to carry out its functions under this Act.

(d) The Committee may conduct such inquiries and investigations as it finds appropriate to carry out its functions under this Act. It may for this purpose request any agency that maintains, or has received, or that is eligible to maintain or receive criminal offender records to produce for inspection statistical data, reports and other information concerning the collection, storage, dissemination and usage of criminal offender record information. Each such agency is authorized and directed to provide such data, reports, and other information.

(e) The Committee shall report annually to the Governor and legislature concerning the collection, storage, dissemination and usage in this state of criminal offender record information. The Governor or legislature may require such additional reports as they deem desirable.

5. Security and Privacy Council.

(a) [The Governor] shall appoint a Security and Privacy Council (hereinafter the Council), consisting of a chairman and not more than eight members, to conduct a continuing study and review of questions of individual privacy and system security in connection with the collection, storage, dissemination and usage of criminal offender record information. In appointing the Council, [the Governor] shall seek such representatives of the general public, state and local government, and the criminal justice community as may be expected to express fairly and vigorously the various interests involved. The Council's Chairman and members shall serve at [the Governor's] pleasure. The Council may appoint and fix the compensation of a staff director, a legal counsel and such other staff personnel as it may from time to time deem appropriate. The Council shall meet at the call of the Governor, its Chairman, or any three of its members to carry out its responsibilities under Section II of this Act, to study the privacy and security implications of criminal offender records, or to formulate recommendations concerning their collection, storage, dissemination or usage. Each Council member shall be entitled to reimbursement for actual and necessary expenses incurred in the performance of official duties.

(b) The Council may conduct inquiries and investigations as it finds appropriate to achieve the purposes of this Act. The Committee, each criminal justice agency in this state, and each state and local agency otherwise authorized access to criminal offender record information is authorized and directed to furnish to the Council, upon request made by its Chairman, such statistical data, reports, and other information as the Council deems necessary to carry out its functions under this Act.

(c) The Council shall report annually to the Governor and legislature concerning both its responsibilities under Section 11 and other questions of privacy and security in connection with the collection, storage, dissemination and usage of criminal offender record information. It may make such additional reports and recommendations as it deems appropriate to carry out its functions under this Act.

(d) The Council may nominate one or more of its members to serve upon any similar council or committee connected with any interstate system for the exchange of criminal offender record information, and may participate when and as it deems appropriate in the activities of any such system.

6. Data Verification and Purging.

(a) The Committee shall adopt regulations creating a continuing program of data auditing and verification to assure the accuracy and completeness of criminal offender record information.

(b) The Committee shall adopt regulations to assure the prompt and complete purging of criminal record information, insofar as such purging is required.

(i) by any statute or valid administrative regulation of this state;

(ii) by the order of any court of competent jurisdiction in this state;

(iii) by the law of any other jurisdiction, where the data or records in question have originated in that jurisdiction;

(iv) to correct any errors shown to exist in such information;

(v) to achieve any of the purposes of this Act, to improve the efficiency of criminal offender recordkeeping, or otherwise to promote the fair and efficient administration of criminal justice.

7. System Security.

(a) The Committee shall adopt regulations to assure the security of criminal offender record information from unauthorized disclosures at all levels of operation in this state.

(b) The Committee shall cause to be initiated for employees of all agencies that maintain, receive, or are eligible to maintain or receive criminal offender record information a continuing educational program in the proper use and control of such information.

8. Access.

(a) Criminal offender record information shall be disseminated, whether directly or through any intermediary, only to (i) criminal justice agencies and (ii) such other individuals and agencies as are, or may subsequently be, authorized access to such records by statute. The Committee shall issue regulations to assure that such information shall be disseminated only in situations in which it is demonstrably required by the individual or agency for purposes of its statutory responsibilities.

(b) It shall be the Committee's responsibility to determine whether each agency requesting access to criminal offender record information is authorized such access under the terms of this Act. The Committee shall, as to each such agency, make a finding in writing of its eligibility or non-eligibility for such access. Except as provided in subsection (c) of this section, no such information shall be disseminated to any agency prior to the Committee's determination of its eligibility or, in cases in which the Committee's decision is appealed under Section 12 of this Act, prior to the final judgment of a court of competent jurisdiction that the agency is so eligible.

(c) For a period of [six months] following the adoption of this Act, or until such time as the Committee completes its determination of the eligibility or non-eligibility for access of a requesting agency, whichever first occurs, any such requesting agency that is receiving criminal offender record information at the time of this Act's passage shall be deemed to be eligible for such access.

(d) Each agency holding or receiving criminal offender record information shall maintain, for such period as is found by the Committee to be appropriate, a listing of the agencies to which it has released or communicated such information. Such listings, or reasonable samples thereof, may from time to time be reviewed by the Committee, Council, or any of their staff members to determine whether this Act or any applicable regulations have been violated.

(e) Dissemination from any agency in this state of criminal offender record information shall, except for purposes of programs of research approved under Section 9, and with the further exception of instances in which a warrant has been obtained in accordance with subsection (f) of this section, be permitted only if the inquiry is based upon name, fingerprints or other personal identifying characteristics. The Committee shall issue regulations to prevent dissemination of such information, except in the above situations, where inquiries are based upon categories of offense or data elements other than name, fingerprints or other personal identifying characteristics.

(f) Notwithstanding the provisions of subsection (e), access to criminal offender record information on the basis of data elements other than personal identifying characteristics shall be permissible if the criminal justice agency seeking such access has first obtained from a (magistrate, judge or justice) a class access warrant. Such warrants may be issued as a matter of discretion by a (magistrate, judge or justice of any court of this state) in cases in which probable cause has been shown that (i) such access is imperative for purposes of the criminal justice agency's investigational or other responsibilities, and (ii) the information sought to be obtained is not reasonably available from any other source or through any other method. A summary of each request for such a warrant, together with a statement of its disposition, shall within ninety days of disposition be furnished the Committee.

9. Research.

(a) The Committee shall issue regulations to govern the usage in this state of criminal offender record information for purposes of programs of research. Such regulations shall require preservation of the anonymity of the individuals to whom such information relates, shall require the completion of nondisclosure agreements by all participants in such programs, and shall impose such additional requirements and conditions as the Committee finds to be necessary to assure the protection of privacy and security interests.

(b) The Committee may monitor any such programs to assure satisfaction both of the requirements of this Act and of any applicable regulations. The Committee may, if

it determines either that such requirements have not been satisfied or that a program's continuance otherwise threatens privacy or security interests, prohibit access on behalf of any such program to criminal offender record information.

(c) Any state or local agency may request the Committee to evaluate any proposed program of research and to offer recommendations concerning its consistency with the purposes and requirements of this Act.

10. Interstate Systems for the Exchange of Criminal Offender Record Information.

(a) The Committee shall regulate the participation by all state and local agencies in any interstate system for the exchange of criminal offender record information, and shall be responsible to assure the consistency of such participation with the terms and purposes of this Act. The Committee shall have no authority to compel any agency to participate in any such interstate system.

(b) Direct access to any such system shall be limited to such criminal justice agencies as are expressly designated for that purpose by the Committee. Where any such system employs telecommunications access terminals, the Committee shall limit the number and placement of such terminals to those for which adequate security measures may be taken and as to which the Committee may impose appropriate supervisory regulations.

11. Rights of Access and Challenge.

(a) Each individual shall have the right to inspect criminal offender record information located within this state which refers to him. If an individual believes such information to be inaccurate or incomplete, he may request the agency having custody or control of the records to purge, modify or supplement them. Should the agency decline to so act, or should the individual believe the agency's decision to be otherwise unsatisfactory, the individual may in writing request review by the Council. The Council, its representative or agent shall, in each case in which it finds prima facie basis for complaint, conduct a hearing at which the individual may appear with counsel, present evidence, and examine and cross-examine witnesses. Written findings and conclusions shall be issued. Should the record in question be found to be inaccurate, incomplete or misleading, the Council shall order it to be appropriately purged, modified or supplemented by an explanatory notation. Each agency or individual in the state with custody, possession or control of any such record shall promptly cause each and every copy thereof in its custody, possession or control to be altered in accordance with the Council's order. Notification of each such deletion, amendment and supplementary notation shall be promptly disseminated by the Committee to any individuals or agencies to which the records in question have been communicated, as well as to the individual whose records have been ordered so altered.

(b) Agencies at which criminal offender records are sought to be inspected may prescribe reasonable hours and places of inspection, and may impose such additional restrictions, including fingerprinting, as are reasonably necessary both to assure the record's security and to verify the identities of those who seek to inspect them.

12. Appeal.

Any individual or agency aggrieved by any order or decision of the Committee or Council may appeal such order or decision to the [trial court] in the county in which he is resident or in which the Council, the Committee, their representative or agent issued the order or decision from which the individual or agency appeals. The court shall in each such case conduct a *de novo* hearing, and may order such relief as it finds to be required by equity.

13. Civil Liability.

(a) Any person may institute a civil action for damages or to restrain any violation of this Act, or both. Should it be found in any such action that there has occurred a willful violation of this Act, the violator shall, in addition to any liability for such actual damages as may be shown, be liable for exemplary damages of not less than one hundred and not more than one thousand dollars for each such violation, together with costs and reasonable attorneys' fees and disbursements incurred by the person bringing the action.

(b) If, in any civil action alleging the publication or dissemination of criminal offender records, it is found that the provisions of this Act or of any regulations issued there-under with respect to the communication or dissemination of such records have been violated, the violator shall not be entitled to claim any privilege, absolute or qualified, as a defense thereto.

14. Criminal Penalties.

Any person who willfully requests, obtains or seeks to obtain criminal offender record information under false pretenses, or who willfully communicates or seeks to communicate criminal offender record information to any agency or person except in accordance with this Act, or any member, officer, employee or agent of the Committee, the Council or any participating agency, or any person connected with any research program authorized pursuant to Section 9, who willfully falsifies criminal offender record information, or any records relating thereto, shall for each such offense be fined [not more than five thousand dollars, or imprisoned in the state penitentiary not more than two years, or both]. Any person who knowingly, but without criminal purpose, communicates or seeks to communicate criminal offender record information except in accordance with this Act shall for each such offense be fined [not more than one hundred dollars, or imprisoned not more than ten days, or both].

15. [Authorization of Appropriations.]

SESSION SUMMARY

The committee heard first from Thomas Madden, General Counsel of the Law Enforcement Assistance Administration, who described the fundamental balance to be struck in these policy determinations:

> Mr. Chairman, in your consideration of the right of privacy and criminal justice information systems it is important that you develop legislation which strikes a proper balance between the legitimate information needs of the criminal justice system and the constitutional rights of citizens affected by this information.
>
> Part of a citizen's right of privacy is lost through engagement in criminal activity. By law or by custom in each state the facts of an individual's arrest, trial and conviction are all matters of public record. Law enforcement agencies maintain police blotters or arrest books which are generally open to the public. Grand jury indictments and records of court proceedings are available to the public in state and local courts.
>
> Legislation must be developed which clearly defines the degree to which a citizen's right to privacy should be further modified by contact with the criminal justice system, particularly where an arrest does not lead to a conviction.

Madden identified the primary issues involved in developing Federal or state legislation as follows:

(a) the administration of the privacy legislation and the noncompliance sanctions in the legislation;
(b) the types of information to be covered;
(c) the types of criminal justice agencies to be covered;
(d) the use of criminal justice information for law enforcement purposes;
(e) the non-criminal justice use of criminal justice information;
(f) accuracy and timeliness of information;
(g) access by the press;
(h) access by individuals for the purpose of review and correction;
(i) sealing and purging; and
(j) security.

Mr. Madden identified five essential types of criminal justice information:

1. arrest information,
2. criminal record information,
3. correctional or release information,
4. criminal intelligence information and
5. criminal justice investigative information.

He stated that different privacy standards are necessary to deal with the collection, dissemination and use of each type of information, and he later discussed the issue of non-criminal justice use of criminal justice information in terms of these classifications. He explained that it is generally agreed that intelligence information should not be made available for any non-criminal justice use or to any non-criminal justice agency except for national defense purposes or the protection of individuals whose lives are in imminent danger. He said that investigative and correctional or release information should be similarly restricted, with the additional possible exception of use essential to effective rehabilitation.

There are, however, according to Madden, legitimate non-criminal justice uses for criminal record information and arrest record information. He suggested that such uses include consideration in the processes of licensing or hiring for certain sensitive positions, but went on to state that only uses authorized by statute or executive order pursuant to statute should be permitted. He stressed that a distinction should be made between arrest records that do not include dispositions and criminal record information.

Another issue of major concern is the accuracy and timeliness of criminal justice information. Mr. Madden observed that the best protection of an individual's privacy may simply be to insure that any information maintained in a criminal justice information system is accurate and that dispositions are recorded in a timely manner so that information disseminated will be an accurate reflection of an individual's criminal history. He said:

> Legislation should require that every item of information entered in a system is checked for accuracy and completeness before entry, and that inaccurate, incomplete, unclear, or ambiguous data should not be entered in a criminal justice information system. Legislation should require that steps be taken to assure that systematic

audits are conducted to be sure that the files are regularly and accurately updated.

Addressing the subject of individual access to criminal justice information, Madden stated that it is generally agreed by those operating and administering criminal justice information systems that an individual should not only have access to both criminal and arrest record information about him contained in the system, but also, in order to assure accuracy, he should have opportunity for challenge and a simple, legitimate way of getting corrections entered. Intelligence information on the other hand, should not be made available because of its sensitivity and the risk of compromising and possibly endangering confidential sources. He noted that similar concern has been expressed about investigative information and correctional records.

Mr. Madden concluded his testimony with a summary of Federal activity and reiterated his belief that law enforcement agencies should be allowed maximum use of criminal justice information for legitimate law enforcement purposes with tight controls and legislative sanctions for proper use of sensitive information.

In response to the question of an attendant, Mr. Madden expressed the opinion that legislation regulating collection, maintenance and dissemination of criminal justice information should be applied to manual recording systems as well as automated systems.

He later stated that he would support legislation authorizing individuals to apply to the court for purging of arrest records containing arrests based on mistaken identity, acquittals, non-prosecuted charges, and similar information, and establishing a fairly simple, inexpensive process that would encourage such applications. However, he expressed opposition to a system of automatic expunging absent individual initiative. He recommended consideration of the issue on a state-by-state basis.

Following Mr. Madden was Archibald Murray, the Director of the New York State Planning Agency for Criminal Justice. In commenting on the Alaska, Iowa and Massachusetts statutes and the Search model legislation, Mr. Murray noted that a common thread was the vesting of most of the rule-making authority in a board or council. He expressed concern that the legislation provided few guidelines and possibly delegated greater discretion in the central agency than is constitutionally permissible.

A second common provision, which Mr. Murray felt was extremely critical, was the grant to the central agency of authority to control participation in interstate information systems. He said:

> Unless that central system has the authority to regulate and therefore to prohibit in appropriate instances the connection between a given locality and an interstate system, I think that state will find that it may be faced with a conglomerate that will very likely violate all of the basic principles that the central information system would normally try and expect to put in place.

On the issue of non-criminal justice use of criminal justice information, Mr. Murray noted a proliferation of statutes authorizing dissemination of information to non law-enforcement agencies and stated:

> In my view, the only rational way of approaching this problem of distribution of criminal history information outside of the criminal justice system is to start off with a comprehensive view of what is meant by the notion of rehabilitation and what it is we as a state or a society expect to accomplish by punishing an individual who has been convicted of a crime. On the one hand, we are likely to say that that individual, having paid his debt, as it were, ought to be restored to full membership in the society. But, on the other hand, wherever the activity in which that person engages somehow or other has some slight degree of delicacy or sensitivity attached, we immediately throw up barriers because of a prior conviction. I think, if we are to bring any degree of semblance of order to the system, we should first decide what are really the legitimate impediments caused by conviction. We should then decide what areas of activity truly are imperiled if a person participates who has a prior criminal history, and then some sort of a circle drawn around that area of activity and only in the case of licensing or employment in that particular limited area should there be authority to use a prior conviction as a bar to participation.

Capsulizing the especially thorny problem of criminal intelligence information, Murray commented:

> I suspect that criminal intelligence information is perhaps the most serious aspect in terms of potential information damage of all the items of information collected with the data banks of this sort.
>
> At least in the instance of criminal history information, one has the option of going back to the police blotter or back to the court dockets or back to the entry registers at the correctional institution to verify whether or not this individual did, in fact, get arrested, was, in fact, convicted, and was, in fact, received in an institution.
>
> Intelligence information, however, by virtue of its very nature, is very often less than complete, very often not verified, very often not verifiable.

Murray expressed the opinion that each of the criminal justice information bills considered in this seminar hearing had failed adequately to deal with the problems of collection, maintenance and dissemination of this type of information, and he recommended that these matters be dealt with and not postponed or ignored. Mr. Murray expressed strong support for the inclusion of a provision such as that in the Iowa statute which imposed a duty upon the court to report disposition information.

The next witness was Mr. Edward J. Kelly, Chairman of the Iowa State Bar Association's Special Committee on Traffic Records and Criminal Information Systems. He opened by stating his disposition in favor of the Iowa statute's vesting the administration of a criminal justice information statute within a commission as opposed to a single individual:

> This commission, as you will be interested in knowing, is composed of two senators selected by the lieutenant governor of the state as the presiding officer; two members of the House of Representatives, selected by the speaker of the house; a judge serving in the District Court of Iowa, selected by the governor; two citizens at large not engaged in any law enforcement activity whatsoever, selected by the governor; and one law enforcement official selected by the governor and the director of public safety.
>
> That gives a board of nine persons charged with the administration and responsibility of this act. We have felt in Iowa that that's a better solution than that suggusted by the other panelists because then you bring to bear the opinions and judgments of a cross-section of the community.

Kelly pointed out that the security of data maintained by law enforcement units is a ticklish problem in rural communities where caretaking of information is less sophisticated than in urban areas, and stressed the need for development of safeguards, especially as technological advances increase the flow of information.

Chairman Quinn questioned Kelly about the privacy implications of newspaper data banks containing criminal history information and the following discussion ensued:

> Kelly: My own personal judgement is that if the newspaper wants to go the expense of keeping a file on you and me, that's their responsibility. They have a right to do that.
>
> Q: How about private organizations setting up their own information systems, simply going to public records and collecting arrest and other criminal history records information, and selling it to employers?
>
> Kelly: I know of nothing in the law that prohibits you from setting up a corporation and buying the necessary hardware and putting on that hardware the information you think is important about any subject. Whether or not it brings on libel or slander or causes you liability is another question.

At another point, Kelly stated that he felt there was no need to differentiate between manual and computerized systems as far as controls and sanctions are concerned.

Strong opposition was voiced in response to the suggestion of one attendant that a Federal agency should be created and charged with responsibility for mandatory collection of all records maintained on individuals and for centralization of this information so that an individual could go to one source to find out about records kept about him. The consensus seemed to be that the potential dangers involved in aggregation of information outweighed the benefit of convenience for the individual.

Mr. Richard Harris, Director of the Virginia State Planning Agency, was the fourth and final witness to testify.

He highlighted several areas of concern he felt must be addressed by legislation regulating collection and use of criminal justice information:

1. Proper and sufficient justification must be

demanded for the collection and storage of criminal justice data.

2. In turn, controls must be imposed on the storage of this data in the system as well as its dissemination and use.
3. A distinction must be made as to the type and classification of information within the system.
4. Provisions must be made for verification of the information collected and stored and for its destruction when obsolete.
5. Questions about an individual's access to his own records with review and correction of inaccurate or incomplete information must be answered.
6. Finally, a determination must be made as to where authority should rest for monitoring the operating procedures of criminal justice information systems at the Federal, state, and local levels.

With regard to the issue of control, Harris stated that, notwithstanding the expenditure of Federal funds for criminal justice data systems, the majority of actual operation and maintenance is at the state and local level and therefore the majority of control should also remain at the state and local level.

Harris emphasized that questions of management techniques and cost effectiveness should not be separated from those of privacy and security, and the relationship among these issues should be addressed by any legislation drafted. He also discussed the issue of the individual's right to review criminal justice records:

> In addition to keeping general administrative records, we feel that agencies operating such criminal justice data systems must be required to maintain records identifying the source of information and to whom it was disseminated. Such a transaction log is useful for at least three reasons. It will notify the individual concerning who received that information about him. It will assist the data bank in easy retrieval of records disseminated and, from a management standpoint, it will allow monitoring of the usage of active files.
>
> Provisions must also be made for the cost of such review and possible challenge. Are we to have some fund set up, as we do for indigent defendants, to provide payment for the challenging at taxpayers' expense and to engage in the expense of litigation and administrative procedures over his particular challenge, assuming for the moment that it occurred? What is going to be the cost-effectiveness of that procedure? Do we have the funds at Federal, State or local levels to provide for that kind of procedure?
>
> Undue burdens should not be placed on the individual by requiring him to seek out the agency responsible for an inaccurate entry. This requirement should rest with the operating agency, as does the responsibility for keeping the data complete, accurate, and up-to-date.
>
> On the other hand, the individual must bear some of the administrative costs of his access and possible challenge to deter unnecessary entry and challenges. It seems to me that there is potential, looking at it from the other side, for disruptiveness on the part of individuals or organizations if they have unlimited rights of challenge.

The discussion centered next on the question of a possible distinction between criminal history files maintained by different branches of government.

> Quinn: We've been talking about criminal history files, and I wonder whether any member of the panel distinguishes between criminal history files kept by the executive branch agencies and those kept by the judicial branch of government, and what relationship, if any, there should be between them.
>
> Harris: Well, my answer is that the criminal history data maintained at the State level should be one set of criminal history data, and it should have within it all the data that's needed by the various divisions of the criminal justice system with the right of each to draw upon those elements of criminal history of the particular individual applicable to their function.
>
> Murray: There is a need for contributions from all elements of the system. The police may supply to your agency the information that an individual has been arrested, but it would certainly be preferable to get information about the ultimate disposition from the court than to get it from the police. Similarly, business about the release of the individual should come from the correctional side.

An attendant raised a question concerning the effect of the separation of powers doctrine on an information system involving the judicial with the executive branch. Chairman Quinn responded that no problem existed in Massachusetts at present, but that the Supreme Judicial Court had been asked whether legislation creating a single computer bank to hold all the data of court personnel, court records, court information, and executive department information would be constitutional. The Court had responded in the negative on the basis of the separation of powers doctrine. An attendant noted that one interesting point made in the opinion was the suggestion of a need for a fourth branch of government related to information services.

Mr. Harris stated that at the outset there must be a clarification of the type of data to be contained in a system, and that the content would depend upon the primary use for which the information is collected and stored. He continued:

> For example, the term "criminal justice intelligence information" must be distinguished from "criminal justice information." A chief difference between the two terms is that the latter is specifically oriented to present criminal justice activity while the former is retained for possible future use. That is, criminal justice information is maintained for general criminal justice agency use and should contain each and every transaction presently pertaining to an individual; whereas, "intelligence" information is specifically oriented to law enforcement agency use and maintained for possible future apprehension and surveillance.
>
> In the intelligence community, analysis is what is done to produce intelligence. What you collect is not intelligence; what you collect is information. It is the analysis of the information that makes it intelligence.
>
> This difference should lead legislative drafters to consider another difference: that intelligence information may not be as fact-oriented and verifiable as criminal justice information. These two considerations may not be true in every case, but are representative.
>
> Thus, provision must be made for the collection and storage of intelligence information, with strict controls placed on its dissemination, and under no circumstances should this type of information be disseminated to non-criminal justice agencies or to private industry.
>
> Access to criminal justice information systems by non-criminal justice agencies and especially private industry must not be allowed, unless by specific statutory authority. If good reason can in fact be provided for allowing certain non-criminal justice agencies access to certain data for specific reasons, stringent restrictions and regulations must be mandated in the legislation.

Harris pointed out that once information has been disseminated from a criminal justice data bank, it is impossible for the disseminating agency or data bank to maintain direct control over the information. He stressed the need for insurance of necessary controls, while recognizing that absolute control is a practical impossibility. While prohibition of direct dissemination of printed information or records is one of the most meaningful controls over secondary dissemination, according to Harris, differing translations, unreliability of verbal communications, possible infringement on an individual's right of review and the impediment placed on law enforcement make this approach impractical. He suggested that one practical solution might be to require the return of all document copies, printed transmittals, and original correspondence to the original sender, with stiff penalties for secondary dissemination and non-compliance.

Harris briefly outlined several steps taken in the State of Virginia in response to the need for control in the production of personal data and the safeguarding of the individual right to privacy:

> The Governor's office has concluded that the executive branch must formulate definitive policies relating to information privacy and security. A full-fledged effort to develop these policies within the next month is now underway. The Governor's cabinet has initiated a special project to aid in the development of an executive policy that will (1) provide an inventory of existing automated information systems in state agencies and of the present practices of those systems relative to information privacy and security; (2) survey the needs of operating agencies, operating constraints and considerations posed by each unique situation; and (3) research alternative methods that might be adapted by an agency to cope with all aspects of privacy and security.
>
> In the legislative branch, two separate study resolutions passed at the 1974 General Assembly will result in the presentation of privacy and security legislative proposals at the 1975 session.
>
> Senate Joint Resolution 10 directed the Virginia Advisory Legislative Council to study and report "on all aspects of the problems involving personal privacy and liberty in the use of computers." The Commission has been charged to "study the experience of other states and make a recommendation concerning the establishment of a privacy and security council in the Commonwealth of Virginia." The VALC has established a committee to study computer privacy and security, which is now well into its examination of public and private personal information systems.

Senate Joint Resolution 63 created a "Comprehensive Criminal Justice Information System Task Force" under the direction of the Virginia State Crime Commission. The Task Force has been directed to "make a full and complete study of all matters relating to the exchange, collection, storage, security, privacy, and use of information in the Virginia criminal justice system" and to "make recommendations as to the development and implementation" of an integrated criminal justice information network. The Task Force has been concentrating heavily on security and privacy controls in the formulation of its recommendations.

This concluded the testimony of Mr. Richard Harris. Following a brief summary by Chairman Quinn of the various issues raised, the session was adjourned.

CHAPTER 3

PUBLIC EMPLOYEE RECORDS

The Chairman of the mock legislative hearings on public employee records was Eric Plaut, M.D., Deputy Commissioner of the Department of Mental Health from the State of Indiana. Committee members included Jerry T. Pierce, State Senator from Oklahoma, and Joan Vollmer, Deputy Commissioner of Personnel for the State of Tennessee. Witnesses before the committee included Gary D. Bearden, Director of the Bureau of Manpower Information Systems of the U. S. Civil Service Commission, Harry B. Douglas, Jr., Coordinator of Equal Employment Opportunity for the State of Florida, and Sheldon Mann, Economist from the Research Department of the American Federation of State, County and Municipal Employees.

Materials sent to all Seminar participants in advance of the meeting included the issue paper reprinted below:

ISSUE PAPER

PRIVACY SAFEGUARDS FOR PUBLIC EMPLOYEES' RECORDS

Frequently, personnel records contain collections of information acquired from many sources and unknown to the individual employee or applicant for employment. This information, often widely shared among officials of the employing organization and with other organizations, is used for a variety of personnel management purposes and to answer queries from creditors, law enforcement agencies, private investigators, recruitment agencies, and prospective employers. These varied uses, in the absence of good information management practices, can constitute a substantial threat to the personal privacy of the individuals about whom personnel records are maintained.

Personnel managers must assure that the personnel management system contains the information needed to carry out their responsibilities effectively; at the same time, they must take all steps necessary to protect the personal privacy of current or prior employees and applicants.

APPLICABLE PRINCIPLES

Five fundamental principles for handling personal information in the files of any record-keeping organization are gaining wide acceptance:

1. There must be no personal data record-keeping operation whose very existence is secret.
2. There must be a way for an individual to find out what information about him is in a record and how it is used.
3. 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.
4. There must be a way for an individual to correct or amend a record of identifiable information about himself.
5. Any organization creating, maintaining, or disseminating records of identifiable personal data must ensure the reliability of the data for the intended use and must take precautions to prevent misuse of the data.

ISSUES

Because it is difficult to specify in advance, and for all time, which items of information may be required to support personnel management processes, the personal privacy of individuals who are the subjects of personnel records cannot be protected simply by proscribing the collection of certain types of data. Nor will data security safeguards alone accomplish the task since the key issues are policy issues: who shall be authorized to use which information for which purposes; under what circumstances; and with what restrictions on further use, disclosure, or dissemination? What is needed, in short, is a well-planned, coordinated program of personnel information management based on the five principles set forth above. In addition, for a personnel information management program to be effective, it is essential that the responsibility for setting and enforcing necessary safeguards rests with top management, that the effectiveness of the safeguards are monitored and periodically evaluated by an audit group, and that sanctions are imposed when procedures are violated.

For state and local government employers, the basic principles, operating rules, audit obligations, and sanctions could be established by legislation, executive orders, or agency regulations. It is probably advisable to treat employee privacy considerations separately through one of these devices rather than within the framework of privacy legislation applicable to general government data banks. In employer-employee matters, government's involvement with the individual goes beyond the relationship of the constituted governing authority to the citizen. Therefore, special treatment in the application of privacy principles is justified. In addition, the kinds of records kept and the services and benefits offered to employees by a government will be basically uniform.*

In any event, once the ground rules have been set, whether by legislation or administration actions, detailed procedures should be developed for controlling the acquisition, retention, and dissemination of information concerning public employees. For the information management program to be most effective, the procedures for collecting, maintaining and disseminating information must be standardized and well documented. Detailed procedures tell users how they are to treat information and give auditors a standard for evaluating user performance.

Ideally, the detailed operating procedures should make clear which items of information individuals are required to provide about themselves, which items they may refuse to provide, and the purpose for which the information is requested. They should provide for a designated point at which user requests for information are received and processed. The procedures should also specify how long information is to be retained; who is allowed to see or to change it and under what circumstances; the security procedures to be adopted to control access to it; and the methods to be used for verifying the accuracy and timeliness of information.

The matter of unqualified access to records by the individual involved does raise questions. For example, should he have full access to medical information, or information supplied in confidence to the employer or prospective employer? Further, access to employee records by others in the employing organization requires careful analysis, depending upon the variety of services or benefits available through the employer and the relationship of the information to employee performance. For instance, who should be able to see whether an employee has taken out a loan or mortgage, has life insurance, or has had checks returned for insufficient funds? To whom are performance evaluations relevant or a list of employee activities or club memberships?

* It can be argued that in the private sector legislation to regulate employee records would be difficult to implement since the configuration of employee records will vary widely in accordance with the nature of the business, the size of the organization and the scope of employee services or benefits provided.

ILLUSTRATIVE LEGISLATION

Also sent to Seminar participants in advance was an illustrative draft bill concerning the protection of public employee rights of privacy, which served as a basis for the Committee's deliberations and is reprinted in full below:

A BILL

To protect the constitutional rights and privacy of individuals who are employed by government and about whom personal information has been collected for personnel management purposes.

TITLE I—DECLARATION OF POLICY: DEFINITIONS

Findings And Declaration Of Policy

SEC. 101. The personnel management missions that are a part of any large government organization require a substantial output of information about individuals and about agency operational programs. This information is required for such purposes as:

1. Determining eligibilty of individuals for employment.
2. Determining physical and mental fitness of individuals for the work required.
3. Setting occupational standards and developing personnel management policies.
4. Evaluating personnel management programs.
5. Maintaining morale and discipline in the work force.
6. Processing grievances and appeals.
7. Determining entitlement to and amount of employment and retirement benefits.

Government agencies must assure that the personnel management system contains operational and personal information necessary to carry out the above purposes effectively, while at the same time taking all the steps necessary to protect the privacy of individual applicants, employees, and retired persons about whom information is maintained.

These agencies must strive to protect the privacy of individuals by controlling the disclosure and use of identifying numbers and indentifiable personal information and assuring the security and accuracy of all steps in the information process. If personal information about an individual is compromised, that individual is compromised.

Definitions

SEC. 102. For purposes of this Act—

(1) "Automated system" means an information system that utilizes electronic computers, central information storage facilities, telecommunication lines, or other automatic data processing equipment used wholly or in part for data collection, analysis, or display, as distinguished from a system in which such activities are performed manually.

(2) "Dissemination" means the transmission of information, whether orally, in writing, or by automated media.

(3) "Personal information" includes all data that (a) describes anything about an individual, such as indentifying characteristics, measurements, test scores; (b) indicates things done by or to an individual, including, but not limited to, records of financial transactions, or medical treatment; or (c) affords a clear basis for inferring personal characteristics or things done by or to an individual, including, but not limited to, the record of his presence in a place, attendance at a meeting, or attendance at some type of service institution.

(4) "Personnel management" means the process of managing personnel programs involving the organized collection of past, present and projected information about operations and personnel for the purpose of planning and controliing those programs.

(5) "Statistical and research purposes" means a use which will not have a direct effect on any specific individual and the principal output of which is based on aggregate data.

TITLE II — COLLECTION AND DISSEMINATION OF PERSONNEL INFORMATION USED FOR PERSONNEL MANAGEMENT

Collection of Personal Information

SEC. 201. The commissioner of civil service will prescribe the basic personal information that shall be collected and used in each personnel management function or process, in accordance with the provisions of this Act.

Each department and agency that wishes to obtain additional personal information beyond the basic information prescribed by the commissioner will be required to justify its need for the additional information.

Justifications of such additional personal information must be based on the following criteria:

(1) Items of personal information sought must be related to specific personnel management processes that are authorized by statute, executive order, or regulation.

(2) The relationship between the information sought and the personnel management purpose to be served must be demonstrated.

(3) The procedures to be employed in collecting, processing, storing, safeguarding, using, releasing, disseminating, and disposing of personal information must be described and must conform with civil service policies and regulations relating to protection of individual privacy.

Personal information needed for personnel management purposes will not be obtained by surreptitious methods or by means that cannot be disclosed to the individuals involved.

Storing, Safeguarding, Processing Personal Information

SEC. 202. Agencies shall take adequate precautions to prevent unauthorized access to personnel management records containing personal information.

This section pertains to records maintained in manual filing systems as well as those in automated systems.

This section requires agencies to set up reasonable combinations of physical security, administrative controls, and technical safeguards to prevent unauthorized access to personal information records, to provide for audits, to permit investigations when unauthorized access does occur, and to identify officials responsible for security of the records.

The agencies shall maintain, among employees responsible for safeguarding and using personal information records a privacy-conscious environment through continual training, audits and test-runs of security measures, and enforcement of rules.

Release of Personal Information for Personnel Management Purposes

SEC. 203. Personal information in personnel records of agencies shall be disseminated to other agencies for authorized personnel management purposes only on a need-to-know basis.

An agency shall disseminate personal information to representatives of other agencies only when they are identified and authorized or certified by agencies to receive it.

An agency shall release personal information to another agency only after determining that the safeguards of the receiving agency for the security of information and procedures for using the data meet the criteria of this Act.

An agency will disclose personal information only on a need-to-know basis to management officials for personnel management decisions, or for personnel management proceedings, or to personal representatives authorized by the individual to see it.

Lists of individuals eligible for appointment or in-service placement will not be checked or compared with lists of individuals affiliated with or active in a political party or a union.

Release of Personal Information for Purposes Other Than Personnel Management

SEC. 204. Personal information that is gathered for personnel management purposes will not be released by the government for purposes other than personnel management, nor released outside normal personnel management organizational channels except with the consent of the individual involved. When personal information is released as required by statute or executive order, the individual shall be notified in writing by the releasing agency.

Agencies shall release personal information only for personnel administration or public policy purposes, and not for commercial purposes or solicitation.

Agencies will release personal information in authorized circumstances only when it has been determined that those receiving the information will safeguard and use it in accordance with the criteria in this Act.

Additional restrictions on disclosure of personal information to organizations or individuals outside the personnel management field are as stated below:

1 Information about disciplinary actions or appeals from personnel management actions that is disclosed to individuals or organizations other than those directly involved in litigating or settling such cases will identify the offenses alleged and corrective actions taken but will not identify the individuals affected without their consent, until completion of all administrative proceedings and appeals.
2 Information about physical or mental disorders of an individual employee will be disclosed only with the individual's consent and only to licensed medical personnel who are professionally qualified to understand it and use it properly.
3 Evaluations of individual work performance of employees will not be disclosed to officials or agencies other than those directly involved in considering the employee for in-service placement except with the consent of the employee.
4 Home addresses or home telephone numbers of employees, or other information about individual employees will not be disclosed except as required by law.
5 Records of legal, financial, medical, or other personal involvements of individual employees will not be disclosed to individuals or organizations outside the official personnel management field.

Use of Personal Information in Statistical Reports and Research Studies

SEC. 205. Agencies will assure that the identity of individuals included in statistical samples or compilations in connection with authorized studies or research projects will not be disclosed, either by means of identifying information or numbers or by means of statistical manipulation to isolate data which can pertain to only one individual in the sample.

When statistical or research qestions are included in questionnaires or forms used in personnel management functions, the individual will be informed whether or not responses to the questions are mandatory.

When personal information is transferred from one organization to another for statistical or research purposes, the organizations concerned shall be required to comply with the provisions of this Act.

Informing Individuals Regarding Information Required

SEC. 206. Individuals who apply for examnations, jobs, in-service placement training, employment benefits, retirement, or other benefits or rights associated with civil service employment will be informed:

1 What personal information is needed to carry out the personnel management process involved.
2 What information will be obtained in addition to that provided by the individual and from what sources.
3 That the information provided by the individual may be checked or verified by comparison with other records held by schools, law enforcement agencies, employers, financial institutions, or other organizations.
4 What measures will be taken to safeguard personal information from unauthorized access or use.
5 That some of the information will be transferred to other organizations and officials for actions and decisions consistent with the purpose for which the individual provides the information.
6 That the individual has the right to know what information is included in records that will be used in making decisions about him or her.

Individual's Access to Personal Information

SEC. 207. Individuals shall be advised upon request what information is in personnel management records about them which will be used in making decisions relating to them.

Agencies shall accept information from individuals to correct, amend, or refute records that are inaccurate or incomplete for the purpose of making decisions about the individuals.

Before individuals are barred from examinations, denied appointment, removed from the service as unsuitable for employment, or are otherwise denied benefits based on information in records about them, they will be afforded an opportunity to challenge the proposed action in an appropriate administrative proceeding. Such challenges may be to the accuracy, reliability, completeness, or relevance of the information on which the proposed action is based.

TITLE III—ADMINISTRATIVE PROVISIONS: REGULATIONS, CIVIL REMEDIES: CRIMINAL PENALTIES

Administrative Provisions

SEC. 301. Any agency maintaining an automated personnel management system containing personal information shall give public notice of the existence and character of its system once each year. Any agency maintaining more than one system shall publish such annual notices for all its systems simultaneously. Any agency proposing to establish such a system, or to enlarge an existing system, shall give public notice sufficiently 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 purposes of the system;
(3) the categories and estimated number of persons on whom the data is maintained;
(4) the categories of data maintained, indicating which categories are stored in computer-accessible files;
(5) the agency's operating rules and regulations issued pursuant to sections 202 and 207, and the agency's policies and practices regarding data information storage, duration of retention of information, and disposal thereof;
(6) the categories of information sources;
(7) a description of all types of use made of information, indicating those involving computer-accessible files, and including all classes of users and the organizational relationships among them; and
(8) the title, name, and address of the person immediately responsible for the system.

Annual Audit

SEC. 302. At least once annually the commissioner shall conduct a random audit of the practices and procedures of the agencies which collect and disseminate personal information to insure compliance with the requirements and restrictions of this Act.

Each personnel management system shall conduct a similar audit of its own practices and procedures at least once annually.

The results of such audits shall be made available to the public by July 1 of each year beginning on July 1 following the first full calendar year after the effective date of this Act.

Civil Remedies

SEC. 303. Any person aggrieved by a violation of this Act shall have a civil action for damages or any other appropriate remedy against any person, or agency responsible for such violation provided he has exhausted the administrative remedies of section 207.

Such person may bring a civil action under this Act in any district court for the district in which the violation occurs, or in any district court in which such Person resides.

Criminal Penalties

SEC. 304. Whoever willfully disseminates, maintains, or uses information knowing such dissemination, maintenance, or use to be in violation of this Act shall be fined not more than $5,000 or imprisoned for not more than five years, or both.

SESSION SUMMARY

Dr. Plaut opened the committee session with comments on historical conceptions of the roles and relationships of public employees that have resulted in policies and guidelines for this group, which differ from those applied to employees in the private sector. For example, the Hatch Act and similar State legislation have regulated the political activities of public employees, and various laws have prohibited or restricted strikes by government workers. Obviously, the relationships between governments and their employees in these as well as other areas are currently undergoing reevaluation and change.

Access to information about public employees is an emerging issue that calls for special consideration in a conference concerned with government record-keeping. In particular, two seemingly conflicting questions need to be addressed:

1. Does the size and power of government require special measures to protect public employees' privacy when records are maintained about them for personnel management purposes?
2. To what extent does the public accountability of the government employee and, in some cases, the potential for abuse of the power delegated to him, call for handling information about him in a different manner from that which would be appropriate in the private sector?

At this point the first witness, Gary Bearden of the U. S. Civil Service Commission, was called upon to testify. Bearden pointed out that the Civil Service Commission, as a personnel management agency for public employees, endorses, in principle, legislation that:

Permits any employee to inspect his own records and to know what information is maintained about him;

Permits an employee to supplement information contained in his record;

Permits the removal of inaccurate information;

Allows the individual to challenge any information used in an adverse action against him; and

Restricts employee record access to those who need the information for the performance of their duties.

Existing Civil Service Commission regulations generally reflect these considerations. However, they do not permit Federal employees to review some information in their personnel records, i. e.

Medical information that could have an adverse impact on an individual, except through a physician of the employee's choice who may disclose and/or interpret medical information to him;

Testing and examination material, the disclosure of which would compromise the competitive examining process;

Reports of suitability or security investigations that would disclose the source of the information; and

Supervisors' appraisals of an employee's potential for a future assignment, although appraisals of past performance are reviewed and discussed with the employee.

The Civil Service Commission believes that these exceptions to the principle of direct subject access to personnel records are justified. The draft bill under consideration provides for no such exceptions. Also, legislation on public employee records should clearly indicate whether an individual is permitted actually to examine his record and make a copy of it. If so, data identifying other individuals should be deleted, such as lists that identify other candidates for a competitive position.

A bill should also specify procedures whereby an employee may supplement his record. The addition of large amounts of material to records in an automated system could create excessive costs and other operating problems. In these instances, the record in the automated system could note the existence and location of supplemental material maintained elsewhere.

The questioning of the witness and the discussion that followed focused on the following issues:

First, as provided in the draft bill, applicants for public employment or related benefits should be informed that personal data they furnish will be verified by comparison with records of other organizations such as educational institutions, law enforcement agencies, or former employers. In response to a comment that this type of checking, in the absence of any reason to doubt the information provided, implies that the applicant is guilty until proven innocent, Bearden mentioned that verification of qualifications is important in a competitive

examination and evaluation process. Verification can identify the few individuals who falsify or exaggerate their qualifications and who thus have unfair advantage over the majority who respond honestly in submitting their qualifications.

There was general agreement that the information verified should be limited to that needed to compare qualifications with job requirements. Bearden pointed out, however, that in the public sector there are statutory requirements for information that do not relate directly to job performance, e. g. information reflecting agencies' participation in equal employment opportunity programs and statistical data to develop profiles of the work force which are used for a variety of personnel management purposes.

Second, justification was seriously questioned for denying a public employee access to his supervisor's appraisal of his potential for new responsibilities. The Civil Service Commission believes that disclosure of this type of appraisal could damage an employee's effectiveness and his relationship with his supervisor in cases where the latter believes that the employee (who may be outstanding in his present job) is not suited for a different type of position.

Third, the principle of giving an individual direct access to his medical records is generally gaining support; thus, there was some reluctance expressed about requiring access through a physician. However, disagreement with this approach was slight, as long as the individual has an opportunity to comment on and/or amend information in his record.

Fourth, the draft bill requires that an applicant for public employment shall be informed that information he furnishes will be transferred to others for use consistent with the purpose for which it was provided. To assure that information is used in accordance with this provision, a public employer should publish notice of all proposed uses of the information, including notice of any organizations or officials who may be recipients of the data.

Fifth, concerns were expressed about the kinds of information about individuals collected and used in connection with suitability or full field investigations for employment in critical-sensitive government positions. These evaluations illustrate the problems associated with balancing the need for information on which to base informed judgments in the selection of high-level public officials with the privacy interests of the individuals involved. Mr. Bearden pointed out that under Civil Service Commission regulations an individual is informed of the content, but not the source, of any information developed through a suitability investigation that is used in an adverse action against him, e.g., information used to deny him a particular job.

Finally, another sticky question concerns the propriety of maintaining records about public employees that may serve legitimately to identify potential problems that could be averted by early intervention, but that raise serious issues of privacy and employee rights. For example, a police officer may submit reports or willingly answer questions about instances where he used force in carrying out his duties. If such reports can be made public, can be used to answer citizen complaints, or can serve as the basis for a suit against the officer or his employer, both the employee and the agency would be less inclined to maintain those records in the absence of statutory or regulatory requirements. Again this situation raises the question of the possible need for data concerning certain categories of public employees who have special authority that would not be appropriate for other types of employees in either the public or private sectors.

Mr. Sheldon Mann, an economist with the American Federation of State, County, and Municipal Empolyers, testified next. He applauded an apparently growing recognition, at least by some public employers, of the need for legislation to protect the employee right of privacy. While acknowledging that the draft bill under consideration contained many of the requisite safeguards, the bill has serious inadequacies from the standpoint of a public employees union. He enumerated four major criticisms of the bill:

1. In several areas the bill appears to focus on the protection of management rights rather than employee rights, e.g. the listing of seven purposes for the collection of information by management.
2. The meaning and intent of numerous provisions is clouded by vague, ambiguous language, e.g. references to "adequate" security precautions and "normal personnel management organizational channels."
3. The bill makes no reference to collective bargaining agreements and procedures which, along with civil service policies and regulations and administrative proceedings, are important components of any process for assuring employee rights. Union contracts should contain employee rights clauses that include provisions for an employee and/or his authorized representative to have access to his personnel file. Any derogatory information included in an employee's record should be brought to his attention and he should have ample opportunity to respond to and to challenge such information.
4. The draft bill devotes insufficient attention to the critical area of the type of information collected and maintained about public employees. Only information directly relevant to job performance should be recorded.

In the discussion following Mann's testimony, general opposition was expressed to the use of psychological testing and polygraphs by employers. Then the group turned its attention to the appropriate roles of legislation, regulation and other procedures, such as collective bargaining, in defining employee rights. The regulatory process provides more flexibility than does legislation for adjusting to changing conditions in many areas; for example, in spelling out what information is considered job-related and appropriately can be collected. Through a rule-making process, proposals concerning the kinds of data to be collected and their intended use would be published and subject to review and comment by any interested party. However, reservations were expressed about allowing legislative language to remain too general in this area; some participants felt that some statutory limitations on data collection were required to safeguard employee privacy adequately.

A question for Mr. Mann concerning his union's position on allowing public access to government employee performance evaluations again raised the issue of balancing public accountability with the privacy rights of these workers. In addition to policemen, both teachers and social workers were mentioned as employees who by the nature of their responsibilities have special authority over others. The discussion revolved around the extent to which, in either the public or the private sector, accountability should rest with the individual employee as opposed to the employing organization and the senior officials who have responsibility for its overall performance.

Most participants believed that government employee accountability to the public is greater and also, in a sense, qualitatively different from that of an employee in the private sector. However, there was little support for public disclosure of individual performance appraisals and general, but not total, agreement that the responsibility for meeting agency obligations should be focused on appointed or elected officials who have public visibility. Increased citizen participation in governmental affairs can contribute to greater responsiveness by public officials.

Another question concerned the problems, including the costs, associated with acquiring employee consent for additional uses of data originally collected for a specific purpose. One possible approach, especially where unionized employees are involved, is to channel requests for consent through representatives of the employees.

Harry Douglas, equal employment opportunity coordinator for the State of Florida, was then called to testify. He endorsed the principles for handling personal data addressed in the issue paper and largely reflected in the draft bill. He noted, however, that modification of some provisions of the bill would be desirable, particularly in relation to existing Florida law and regulations. He discussed the State's "sunshine" law, adopted in 1967, which requires that meetings of public bodies in the State be open, virtually without exception. He also described an older public records law under which all public documents, except six kinds specifically exempted, are open to scrutiny by any citizen of the State. Currently, there is no exemption for personnel records of public employees, although a pending amendment to the law seeks to establish some re-

strictions on the use and dissemination of some information, including government worker performance evaluations and some background data.

Douglas also advanced the concept that there may be no real conflict between maximum government openness and the protection of personal privacy. A government that is inhibited from engaging in secret activity and maintaining secret records is more likely to engender public trust and cooperation. If its records are open, there may be an incentive to restrict collection of information to that which is necessary for a specified purpose and to avoid the acquisition of data of questionable veracity from questionable sources; the openness may promote a greater sensitivity to individual privacy. Further, if a public agency is operating "in the sunshine," improper official use of information is less likely.

Douglas acknowledged that this approach is not without flaw and that there are risks of both inadvertent and deliberate misuse of publicly available information about individuals. As discussed earlier, the question of making employee performance evaluations available to the public presents a classic dilemma, largely because of the subjective nature of such assessments. Still, as noted, there is an argument favoring public accountability of performance.

The suggestion that maximum openness can lead to maximum assurance of personal privacy incited some lively discussion with various degrees of disagreement as to the validity of the concept, particularly where personnel records are concerned. Douglas stated in response to an inquiry, that he was unaware of any instance where a public employee in Florida had been adversely affected by the disclosure of employment-related information. The employee does have due process rights to appeal whenever he feels his rights have been violated.

Some concern has been expressed about the use of information gained from public employee records and a statutory amendment to place some limitations on dissemination of data is under consideration. In addition, a Court of Appeals decision, relating to the State University system's regulation of access to employee records is pending and could affect record-keeping practices throughout the State personnel system.

Several specific questions and comments were raised in connection with the concept of "open" records across-the-board, e.g.;

> If examinations used for competitive placement or promotion are disseminated publicity, the development and validation of new tests would be very costly.
> An effort to avoid unnecessary or detrimental entries to an employee's record could lead to a failure to record information that should be in an adequate personnel file. Thus, it is important to define, as precisely as possible, appropriate job-related information.

A central and continually recurring issue concerns determination of the need to know in various phases of the personnel management function. Some delineation of the kinds and amounts of information that should be collected and to whom it should be available can be made through the legislative and rule-making processes; however, there will always be requests for data that will have to be handled on an individual basis.

The session ended with agreement among the participants that the draft bill considered by the group served only as a basis for discussion; it was neither endorsed as a model nor appropriately modified. Further discussion of privacy issues and an exchange of relevant legislative and/or administrative proposals among public personnel officials and others concerned with public employee records is clearly needed. The participants recommended specifically that a summary of this session, as well as notice of any future conferences concerning the privacy rights of public employees, be widely distributed to State and local government personnel officials.

CHAPTER 4

STATE AND LOCAL GOVERNMENT DATA BANKS

Stanley J. Aronoff, State Senator from Ohio, served as Chairman of the mock legislative hearings on State and Local Government Data Banks. Witnesses included State Representative William R. Bryant, Jr., of Michigan; Assemblyman Mike Cullen, Chairman of the California Assembly Committee on Efficiency and Cost Control; Daniel B. Magraw, Assistant Commissioner of the Minnesota Department of Administration; and Marjorie Eltzroth, Executive Director of Governor's Privacy Commission, who substituted for Governor Francis W. Sargent of Massachusetts.

The Committee, composed of a cross section of State legislators, other State government officials, and representatives of Federal government, local government, the private sector and the press, received in advance of the Seminar the issue paper reprinted in full below:

ISSUE PAPER

GENERAL DATA BANK LEGISLATION FOR STATE AND LOCAL GOVERNMENT

General legislation on the personal-data record-keeping practices of state and local government agencies can be both the starting point and the backbone of a state's efforts to construct a comprehensive framework of safeguards for personal privacy. Once established in general legislation, basic individual rights as well as obligations of government record-keeping organizations can be reaffirmed, strengthened, extended, or modified in other statutes and in implementing regulations. Drafting such legislation, however, is not easy. There are no models to follow, and expert advice is not only difficult to come by but may vary considerably.

A number of issues and options should be considered by sponsors and drafters of general data bank legislation. They do not pretend to be prescriptive or to exhaust its subject, but hopefully will provide helpful insights and suggestions.

FAIR INFORMATION PRACTICE AND PERSONAL PRIVACY

In drafting any data bank legislation, one should be aware that safeguards against record-keeping invasions of personal privacy are now widely considered to involve much more than prohibiting unauthorized uses and disclosures of personal information. Guaranteeing an individual the right to see, copy, and challenge recorded information about himself has come to be considered an important privacy safeguard equal with the principle that an individual's consent should be obtained before using information about him for any purpose other than that for which it was originally collected.

The core premise of much recent privacy legislation is that policies and practices governing the collection, use, and disclosure of personal information should stress accuracy, judicious use and fairness, and that the best way to meet those objectives is to give the individual a significant opportunity to participate in determining what is recorded about him and with whom it is shared. Effective general legislation, in other words, will seek to assure adherence to at least five basic principles of fair information practice:

1. There must be no personal data record-keeping operation whose very existence is secret.
2. There must be a way for an individual to find out what information about him is in a record and how it is used.
3. 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.
4. There must be a way for an individual to correct or amend a record of identifiable information about himself.
5. Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for the intended use and must take reasonable precautions to prevent misuse of the data.

It will be noted that these principles do not provide the basis for determining *a priori* which data may or may not be recorded and used, or why and when. However, they do provide a basis for establishing procedures that assure individuals, singly or collectively, the right to participate in a meaningful way in decisions about what goes into records about them and how that information will be used.

INITIAL POLICY DECISIONS

There are many different ways of assuring adherence to fair information practice principles, but the choice of means will be influenced to a substantial degree by a handful of initial decisions about the structure and coverage of draft legislation. For example, if one opts for a central regulatory approach (such as a board or commission with broad oversight and rule-making authority), details normally dealt with in statutory language may sometimes be left to the drafters of implementing regulations. This approach, however, can be costly (in money, personnel, and delayed administrative action) and might turn out to be more effective than legislation that, if painstakingly drafted, would give record-keeping organizations clear guidance on what is expected of them and provide individuals with effective civil remedies in the event they are injured by an organization's failure to live up to its obligations.

It is important to decide at the outset whether and to what extent proposed legislation is to cover any private sector organizations, such as government contractors and grantees. It appears that any attempt to reach out to the private sector in general legislation can present major and perhaps debilitating obstacles, particularly where private organizations are engaged in interstate transactions, or where the legislation makes a violator of any of its requirements vulnerable to criminal prosecution, or where private sector record-keeping organizations are already subject to fair credit reporting legislation.

There also appears to be little reason to distinguish between manual (paper or microfilm) records and records in computer-accessible form. Wholly automated record-keeping systems, i.e., systems where no paper or microfilm record is kept at any point between data collection and data use, seem to be extremely rare, and it appears that there are no noteworthy differences between manual and automated record-keeping policies and practices.

With regard to statistical-reporting and research records, suspending the individual's access, review, and correction rights usually seems sensible and justifiable. The appropriate protection for such records is immunity from subpoena which assures that they will not be used to make a determination about the individual. Moreover, permitting an individual to make changes in a *bona fide* statistical or research record about himself will usually have no practical consequence, save to risk that the record will be rendered useless for analysis. And further, if individuals are guaranteed access to statistical-reporting and research records about themselves, all such records must be maintained in a way that makes them easily retrievable in individually identifiable form, thereby increasing the risk of misuse.

On the question of individuals v. legal entities, residents v. non-residents, and minors and incompetents v. adults and legal guardians, guidance will presumably be sought in other statutes and in pertinent constitutional provisions and court decisions. One approach to the scope question is to have the legislation apply to systems of records from which information about individuals is retrieved (rather than retrievable) by reference to the name, number, or some other identifying feature (such as fingerprints) associated with each individual. This would exclude all records that are indexed and retrieved only by reference to the name of an organization or other legal entity, but would probably not exclude sole proprietorships and partnerships. Hence, a preliminary study might still need to be made of the effect of the proposed legislation on existing statutes that mandate public disclosure of certain information about individuals engaged in various activities that a state regulates or otherwise monitors.

BASIC REQUIREMENTS

Most general data bank legislation has at least five principle parts: one establishes the individual's right to see, copy, review, and challenge a record about himself; another imposes certain minimum obligations on record-keeping organizations; a third deals with authorized disclosures; a fourth stipulates the permissable exemptions; and a fifth establishes civil remedies and criminal penalties. Some bills also contain a sixth part establishing a central administrative and appeals authority and, in a few cases, a central rule-making authority.

Each of these principal subdivisions tends to have certain recognizable features, even though the exact language may differ from bill to bill. Each also has its particular drafting pitfalls. The key features of each section and some typical policy and drafting dilemmas are briefly discussed below:

Rights of Individuals. Conceptually, this section may seem the least complicated of all. Its principal objectives are to guarantee each individual the right to establish that a record-keeping organization does in fact maintain a record about him; to see and copy it in a form that he can understand (i.e., decoded if the record is kept in machine-readable form); to challenge the accuracy, relevance, timeliness, and completeness of information in such a record; and to find out who has had access to it and for what purposes. As a drafting matter, however, experience suggests that it is extremely useful, if not imperative, to keep clearly in mind how each of these rights will actually be exercised.

How, for example, does an individual establish that a record is being kept about him? Should the individual be able to see, copy, and challenge all information in such a record—information about his health and psychological well-being—information pertaining to others who are also named in the record—information provided by a third party which, if disclosed, would reveal the identity of the third party?

Suppose the individual claims that information in the record is inaccurate, outdated, irrelevant, or incomplete. Whose judgment should prevail? Who should be required to verify what? If the differences cannot be resolved, what recourse should the individual have? What about the period during which the record is being contested? Should the individual be able to insert a statement in the record setting forth his version of the facts? How long should such a statement be retained? Should it automatically follow the record wherever it goes or should its existence simply be noted in the record so that a user can request it when needed?

Should the record-keeping organization keep an accounting of all accesses and disclosures, including those to officers and employees of the record-keeping organization who use the records in performing their official duties?

Not all of these considerations can or should be addressed in the statute lest they lock record-system managers into particular administrative approaches or otherwise impede the normal development of imaginative, least-cost solutions to the many practical problems that any legislation of this sort, no matter how carefully drafted, is bound to create. But all of them need to be borne in mind in drafting the pertinent provisions.

On balance, a good drafting approach seems to be to reach for statutory language that makes clear the objective of each provision and closes as many loopholes as can reasonably be anticipated, but also gives those who will have to administer the statute as much procedural (and for computerized systems, as much design) flexibility as possible. This, of course, is the counsel of perfection, but the chances that it will at least be approximated seem far greater when a general data bank statute is drafted with its practical administrative consequences clearly in mind.

Obligations of Record-Keeping Organizations. The usual objective here is to assure that each record-keeping organization to which the legislation applies assumes a proper share of the responsibility for seeing that fair information

practice principles are faithfully observed. Recognizing that an individual cannot ask to see a record that he does not know exists, it usually contains one or more notice provisions.

Commonly there is a provision which requires that individuals asked to provide information about themselves be told why they are being asked, under what legal authority, whether they can refuse to answer, what will happen if they do refuse, and what uses will be made of any information they provide. In this provision, and in the general public notice discussed below, the data collector should be prompted to be as specific as possible in describing purposes and anticipated uses. Since simple assurances that information will be kept confidential have no reliable significance, they should be eschewed in favor of statements that identify and, if possible, describe in some detail all proposed uses.

In addition to statements to individuals at the time inquiries are made of them, general data bank legislation typically requires some form of general public notice that attests to the existence of each personal data record-keeping system to which the legislation applies, describes its principal characteristics, and outlines the steps an individual must take to find out if a record is being kept about him, what information it contains, and the procedures for challenging its accuracy, relevance, timeliness, and completeness.

Without some form of current and widely disseminated general notice, many individuals will not know where and how to exercise the rights that the legislation guarantees them.

Other obligations typically imposed on record-keeping organizations include a requirement that they issue implementing regulations (if they are public agencies); keep an accounting of all disclosures to outside persons (except perhaps to members of the public under public records statutes); and maintain their records with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any decision about an individual made on the basis of information contained therein. The rule-making requirement can give a record-keeping organization the opportunity to establish reasonable times, places, and fees to be charged for making records available to individuals who ask to see them, to establish special procedures for apprising an individual of medical and psychological information in a record about himself, to distinguish between the accesses and disclosures for which a detailed accounting will be kept and those for which some less complicated procedure will be devised, to settle on its procedures for dealing with challenge to information in its records and to make such other adjustments as it may think necessary to comply fully but intelligently with the legislation's basic requirements.

To expect a record-keeping organization to meet some absolute standard of accuracy totally unrelated to the uses to which its records are put could well be regarded as an irresponsible, and certainly an unduly costly demand. However, it is often thought useful to require a record-keeping organization to make certain that any information it actually uses in making a decision about an individual is as accurate, relevant, timely, and complete as is necessary to assure that the information itself does not cause an unfair decision to be made. Such a requirement should work very well so long as all the users of information in a record are subject to the same accuracy-at-point-of-use requirement.

Where it may not suffice, and thus where some additional safeguards may be needed, is where information from a record is disclosed to some organization or individual that is not subject to to the legislation and also not able to guarantee that the information will not be used irresponsible.

Conditions of Disclosure. If a State already has a consistent and well-executed body of laws governing the transfer and disclosure of recorded personal information, it may be well-advised to draft general data bank legislation that does no more than establish an general notice requirement and guarantee individuals the right to see, copy, and correct their records. However, if it does seem desirable to establish a clearly articulated transfer and disclosure policy, a general data bank statute can be the place to do it.

The principle that an individual's consent should be obtained before divulging information in a record about him is the backbone of a responsible transfer and disclosure policy. Yet if that principle had to be followed to the letter in all cases, most government organizations and many private ones would not be able to function. Clearly one must begin to entertain exceptions the moment the individual consent principle is asserted. But for whom and under what circumstances?

Generally, there are three reference points in drafting a "conditions of disclosure" section:

1. Existing so-called "confidentiality" statutes that forbid or otherwise limit certain types of disclosures.
2. Existing public record statutes that mandate certain disclosures.
3. What one might call the "threshold requirements" to be applied in cases where information transfers and disclosures are not covered by an existing statute or where existing statutes are being superseded.

The principal policy issue raised by the first two is whether to amend the existing statutes, either by making it clear that the disclosure conditions in the general data bank legislation are intended to supplant or modify them, or to reaffirm them through the insertion of a savings clause ("Nothing in this section (or Act) shall be construed to affect . . ."). The choice will no doubt be made somewhat differently in each state, although the need to take account of existing federal requirements (such as the confidentiality provisions of the Social Security Act and regulations issued thereunder) will produce some uniformities. The key point, however, is that the decision to overturn or reaffirm existing law should not be made lightly lest a purported "privacy" statute turn out in practice to be a substantial stimulant to the free (i.e., without-consent) disclosure and circulation of personal information.

The third reference point, the threshold issue, is equally delicate because it involves the establishment of "need to know" policies with supporting authorization and documentation requmirements. One wants to be sure to provide for regular, day-to-day access to records by officers and employees of the record-keeping organization who need such access in order to perform their official duties. Presumably one also does not want to impede unnecessarily the work of statisticians and researchers or to place inappropriate constraints on legitimate law enforcement access to records.

Some provision may be needed to cope with emergency situations where the best interests of the record subject would be served by permitting some outside person to have access to a record about him and one can doubtless think of other types of without-consent disclosure that will need to be provided for, including, perhaps, disclosures that facilitate legislative oversight of executive agencies.

No matter what categorical exceptions to the individual consent principle are proposed, how requests for access to records are required to be documented, and what type of official assent is required before access to a record can be given or information disclosed from it (should the head of a government agency be allowed to delegate his power to authorize certain disclosures?), there will probably be a sizeable class of transfers and disclosures for which there appears to be no reason to suspend the individual consent requirement save the fact that not to do so would create an administrative nightmare. Usually these are disclosures that take place frequently, involve large numbers of records, and are clearly necessary to the performance of statutorily authorized government functions. In these cases, a reasonable solution would seem to be to exempt the transferring or disclosing record system from the requirement to obtain an individual's explicit consent to each such transfer or disclosure of information about him, on the condition that he be told of such "routine" uses when he is asked to provide information about himself and that, in addition, each such use will be clearly identified and described in the system's general notice. However, if record-keeping organizations are permitted or required to up-date their public notices periodically, some further provision may be needed to assure that routine uses are not casually established.

Exemptions. It is likely that hearings on draft legislation will identify fair information practice requirements other than the individual-consent-to-disclosure requirement from which it may seem advisable to exempt particular record systems or portions of them. Indeed, it may well be decided that whole categories of record-keeping systems, such as on criminal justice information and public employee personnel, should be dealt with in separate, specially tailored legislation or executive orders. If this is in fact decided, a section on general and specific exemptions will be necessary and a mechanism will have to be found for making them.

One approach is to provide blanket statutory exemptions for certain categories of records, such as those maintained by criminal justice agencies, and to allow agency heads to exempt other types of records or portions of records from specifically enumerated requirements through a public rule-making process. Candidates for the latter type of discretionary, requirement-specific exemptions may include portions of records or record systems where disclosure would very likely identify a source to whom confidentiality was expressly promised, or where data are required by law to be used only for statistical reporting and research. The key questions to be decided will include whether certain types of records or record systems should have an exemption at all and, if so, which kind; whether the rule-making route to obtaining discretionary exemptions should involve a public hearing and an opportunity for court review of the final determination; and, most important, from which requirements exemptions should be permitted.

The answers to these questions will vary depending on the types of records and record systems to be covered by the statute and the prevailing state procedures for public rule making.

However, in all cases it should be hoped that the exemption procedure would be one that modifies rights or permits deviations from organizational obligations only when it is clear that some significant individual interest will be served or that some paramount societal interest can be persuasively demonstrated.

Remedies. The choice between civil and criminal remedies, or some combination thereof, is another that will obviously vary from state to state. If civil remedies are preferred, however, some will probably press for a liquidated damages provision along with the opportunity to recover for actual injury. Opinion may also be divided on whether record-keeping organizations should be vulnerable to civil suits for privacy safeguard violations that do not result in actual injury to an individual or for violations that do not result from arbitrary, willful, or capricious conduct. Of particular importance in fashioning a remedies provision will be the continued existence of public records statutes that penalize withholding rather than disclosure of personal information. Care must be taken to see that conflicting privacy and public information requirements are reconciled.

ILLUSTRATIVE LEGISLATION

The committee received in advance and considered four bills as guides: proposed legislation from the States of California, Michigan and Minnesota, as well as the model bill of the National Association of State Information Systems (NASIS). Only the Minnesota bill had been passed into law (Minn. Stat. 1974, Sec. 15.162). The committee was also advised of pending legislation in Massachusetts and of an executive order in that State. The bills from California, Michigan and NASIS as well as an amended version of the Minnesota bill are reprinted below:

CALIFORNIA LEGISLATURE—1975–76
REGULAR SESSION

ASSEMBLY MILL No. 150

INTRODUCED BY ASSEMBLYMAN CULLEN
DECEMBER 4, 1974

REFERRED TO COMMITTEE ON JUDICIARY

An act to add Title 1.8 (commencing with Section 1798) to Part 4 of Division 3 of the Civil Code, relating to personal data, and making an appropriation therefor.

LEGISLATIVE COUNCIL'S DIGEST

AB 150, as introduced, Cullen (Jud.). Personal data.

While existing law requires that any contract entered into by the Department of Finance, any state agency or any consolidated data center, concerning data processing systems design, programming, documentation, conversion, and other aspects of data processing operations shall contain a provision requiring the contractor and all of his staff working under such contract to maintain all information obtained as a result of such contract as confidential and not to divulge such information to any other person or entity, the existing law contains no general safeguards or restrictions upon obtaining, using, or disclosing personal data contained in information systems or systems of records.

This bill does the following:

(a) Makes legislative declaration that in view of the constitutional right of privacy it is necessary that procedures be established to govern disclosure and use of records containing information about an individual in identifiable form, to afford an individual of the content of such records, and to prohibit any recording, disclosure, or use of personal information not governed by such procedures.

(b) Prohibits disclosure of personal information contained in any personally identifiable record except pursuant to a written request by or with prior written consent of the individual to whom the information pertains, with specified exceptions.

(c) Requires persons maintaining such records, among other things, to keep an accurate accounting of the date, nature and purpose of each disclosure, and the name and address of the person, organization, or agency, to whom disclosure is made.

(d) Requires governmental bodies maintaining automated personal data systems to file annual notice with the Secretary of State specifying, among other things, the nature and purpose of the system and the categories of data to be maintained, and the categories of persons on whom data are maintained. Provides civil penalty for failure to file required report.

(e) Provides cause of action for damages or for an injunction against responsible parties, as specified, for noncompliance with the act.

(f) Makes it a misdemeanor for an unauthorized person to use, obtain, or attempt to use or obtain personal information subject to the requirements set forth herein; and makes it a misdemeanor to knowingly and willfully disclose information in violation hereof.

(g) Exempts specified record and information systems from the prohibitions hereof, including law enforcement records, as specified, and certain public records.

(h) Determines that no relevant evidence relating to any procedure established or required by the act is to be privileged in any civil action for evidentiary purposes, including discovery procedures or other aspects of any cause of action.

(i) Appropriates an unspecified amount of the State Controller for allocation and disbursement to local agencies for costs incurred by them pursuant hereto.

Vote: ⅔. Appropriation: yes. Fiscal committee: yes. State-mandated local program: yes.

The people of the State of California do enact as follows:

SECTION 1. Title 1.8 (commencing with Section 1798) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.8 CALIFORNIA FAIR INFORMATION PRACTICE ACT OF 1975

CHAPTER 1. GENERAL PROVISIONS

1798. This act shall be known and may be cited as the California Fair Information Practice Act of 1975.

1798.1. Recognizing that the right of privacy is a personal and fundamental right granted and secured directly by the Constitution of the State of California, and that the constitutional right of individuals to personal privacy is directly affected by the kind of disclosure and use made of identifiable information about them in a record, and that in order to secure and protect the right to personal privacy of individuals under the Constitution and to enable them to better obtain the enjoyment of such right under Article 1, Section 1, of the Constitution of the State of California, it is necessary that [a] a record containing information about an individual in identifiable form must be governed by procedures that afford the data subject a right to know what the content of the record is or will be, and what disclosure and use will be made of the identifiable information in it; and [b] any recording, disclosure, or use of personal information not governed by such procedures must be prohibited as an unfair information practice unless such recording, disclosure, or use is specifically authorized by the data subject or by statute. It is therefore desirable and appropriate that the Legislature provide for such procedures in law because: The right to privacy is a personal and fundamental right protected by the Constitution of the State of California; the privacy of a data subject may be directly affected by the collection, maintenance, use, and dissemination of personal information; the increasing use of computers and sophisticated information technology, while essential to the efficient operations of government and of private industry, has greatly magnified the potential for harm to individual privacy that can occur from any collection, maintenance, use, and dissemination of personal information; the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections may be endangered by the misuse of certain information; and in order to protect the privacy of data subjects identified in information systems, it is necessary to establish principles relating to the collection, maintenance, use, and dissemination of information by such systems.

Accordingly, the Legislature recognizes basic principles of information systems and practices, pertaining to both automated and manual systems as follows:

(a) There must be no information systems or system of records containing personal information whose very existence is secret.

(b) There must be a way for a data subject to find out what personal information about him is in a record and how it is used.

(c) There must be a way for a data subject to prevent personal information about him obtained for specified purposes from being used or made available for other purposes without his consent or knowledge.

(d) There must be a way for a data subject to correct or amend a record containing personal information about him.

(e) Any agency, organization, or individual creating, maintaining, using, or disseminating records containing personal information must take reasonable precautions to ensure the reliability of the data for their intended use and to prevent misuse of the data.

1798.2. As used in this title:

(a) The term "organization" means an individual, partnership, corporation, association, local public entity, the state, or other group, however organized.

(b) The term "agency" means any office, subdivision, branch, division, or arm of government in California, including state government as well as all other legally constituted governmental organizations in the State of California, except the federal government.

(c) The term "individual" means a natural person.

(d) The term "record" means any collection or grouping of personal information about a data subject that is maintained by an organization, agency, or individual and that contains his name, or an identifying number, symbol, or other identifying particular assigned to the data subject.

(e) The term "information system" refers to a system from which information can be retrieved by the name of the data subject, or by some identifying number, symbol, or other identifying particular assigned to the data subject and includes all processing operations, from initial collection of data through all uses of the data, including outputs from the system. Data recorded on questionnaires, or stored in microfilm archives shall be considered part of a data system.

(f) The term "system of records" means a group of any records under the control of any organization, agency, or individual from which information can be retrieved by the name of the data subject or by some identifying number, symbol, or other identifying particular assigned to the data subject.

(g) The term "statistical research and reporting system" means an information system or a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual.

(h) The term "data subject" means an individual whose name or identity is maintained in an information system, a system of records, or a statistical research and reporting system.

(i) The term "personal information" includes all data that can be associated with identifiable individuals, and [1] describes anything about an individual, such as identifying characteristics, measurements, test scores; [2] indicates things done by or to an individual, including, but not limited to, records of financial transactions, medical treatment, or other services; or [3] affords a clear basis for inferring personal characteristics or things done by or to

an individual, including, but not limited to, the mere record of his presence in a place, attendance at a meeting, or admission to some type of service institution.

(j) The term "unfair information practice" means a failure to comply with the requirements of this act.

(k) The term "maintaining" includes collection, maintenance, or use.

(l) The term "disclosure" means the act or an instance of divulging, revealing, or otherwise opening to view.

(m) The term "disseminate" means to disclose, release, transfer, or otherwise communicate information orally, in writing, or by electronic or other means.

(n) The term "accounting" means to keep a complete, accurate, and up-to-date chronology of disclosures of personal information.

CHAPTER 2. REQUIREMENTS

1798.3. No ogranization, agency, or individual shall disclose any personally identifiable record or any personal information contained in such record by any means of communication to any other organization, agency, or individual, except pursuant to a written request by, or with the prior written consent of the data subject to whom the record or personal information pertains, unless disclosure of such information or record is as follows:

(a) To those officers and employees of the organization or agency maintaining the record who have a need for such record in the performance of their duties.

(b) To a recipient who has provided the organization or agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is transferred in a form that is not individually identifiable.

(c) To the State Archives of the State of California as a record which has sufficient historical or other value to warrant its continued preservation by the California state government, or for evaluation by the Director of General Services or the Archives or his designee to determine whether the record has such value.

(d) To another agency or to an instrumentality of any governmental jurisdiction within or under the control of the State of California for a law enforcement activity if such activity is authorized by law and if the head of such agency or instrumentality has made a written request to the organization or agency which maintains the record, specifying the particular portion desired and the law enforcement activity for which the record is sought.

(e) Pursuant to a showing of compelling circumstances affecting the health or safety of a data subject, if upon such disclosure notification is transmitted to the last known address of such data subject.

(f) To federal, state or local government when such disclosure is authorized or required by law.

1798.4. Each organization, agency, or individual, with respect to each information system or system of records under its control, shall do the following:

(a) Keep an accurate accounting of the following:

[1] The date, nature, and purpose of each disclosure of a record, or portions of a record containing personal information to any other organization, agency, or individual made pursuant to Section 1798.3 except subdivisions (a), (b), (c), and (f) of Section 1798.3 or disclosures to the public from records which by law or regulation are open to public inspection or copying.

[2] The name and address of the organization, agency, or individual to whom such disclosure is made.

(b) Retain the accounting made pursuant to paragraph (1) for at least three years after the disclosure for which such accounting is made.

(c) Except for disclosures made pursuant to subdivision (d) of Section 1798.3 make the accounting made pursuant to paragraph (1) available to the data subject named therein at his request.

(d) Inform any organization, agency, or individual about any correction, amendment, or notation of dispute made by the organization in accordance with subdivision (d) of Section 1798.5 of any record that has been disclosed to such organization, agency, or individual, within two years preceding the making of such correction or amendment of the data subject's record, except that this paragraph shall not apply to any record that was disclosed prior to the effective date of this section.

CHAPTER 3. ACCESS TO RECORDS

1798.5. Each organization, agency, or individual maintaining an information system or a system of records containing personal information shall do each of the following:

(a) Permit access by any data subject upon proper identification to any record or portion thereof containing information pertaining to him which is contained in any such system and permit the data subject to review such record and have a copy made of all or any portion thereof in a form reasonably comprehensible to him.

(b) Permit such data subject to request correction or amendment of a record pertaining to him; and either

[1] Correct or amend any portion thereof which the data subject believes is not accurate, timely, or complete, or;

[2] Promptly inform such data subject of its refusal to correct or amend such record in accordance with his request, the reason for such refusal, the procedures established by the organization, agency, or individual for the data subject to request a review of that refusal, and the name and business address of the official within the organization or agency to whom the request for review may be taken.

(c) Permit any such data subject who disagrees with the organization or agency's refusal to correct or amend his record to request review of such refusal by the official named in accordance with subdivision (b) (2); and if, after such review, that official also refuses to correct or amend the record in accordance with the request, permit the data subject to file with the organization or agency a concise statement setting forth the reasons for his disagreement with the refusal.

(d) In any disclosure containing information about which the data subject has filed a statement of disagreement occurring after the filing of such statement under paragraph [3], clearly note any portion of such information which is disputed. Upon request of either the data subject or the recipient of the information, provide copies of such statement. If the organization or agency deems it appropriate, provide copies of a concise statement of the reasons for not making the corrections or amendments requested.

1798.6. The organization, agency, or individual may charge the data subject a reasonable fee, not the exceed five dollars ($5), for making copies of his record.

1798.7. Each organization, agency, or individual maintaining an information system or system of records shall inform each data subject whom it asks to supply information, at the time the information is requested of the following:

(a) The routine or usual recipients or users of the information.

(b) The principal purpose or purposes for which the information is intended to be used.

(c) Other purposes for which the information may be used.

(d) Which statutes or regulations, if any, require disclosure of such information.

(e) The effects on him, if any, of not providing all or any part of the requested information.

1798.8. Every organization, agency, or individual maintaining one or more automated systems containing personal information shall give notice of the existence and character of each system once each calendar year prior to January 31 of that calendar year, commencing with the calendar year 1977. Such notice shall be filed with the Secretary of State, and shall be a permanent public record. The secretary may establish regulations prescribing the form of such notice to implement this subsection, and may charge a filing fee not to exceed five dollars ($5) for each notice filed to defray the administrative costs incurred pursuant to this section. Any organization, agency, or individual maintaining more than one information system or system of records containing personal information may file such annual notices for each of its systems simultaneously, and such notices may be combined as a single filing when appropriate. In this regard, where a single system is duplicated or repeated at more than one location, under the guidance of a central office, such system may be reported as a single system, specifying each location where it is operated and where files exist which contain personal information. Any organization, agency, or individual proposing to establish a new information system or system of records, or to change the personal information content of an existing system, on or after the effective date of this subsection, shall file a notice with the secretary within ninety (90) days of establishing or changing the personal information content of such system. Notices shall specify each of the following:

(a) The name of the system and the name and address of the organization, agency, or individual maintaining the system.

(b) The nature and purpose of the system.

(c) The categories of persons on whom data are or are expected to be maintained.

(d) The categories of data to be maintained, including, but not limited to, financial, personal health, education, and property data.

Notwithstanding any other provisions of this title, every person who fails to file a notice as required by this section shall be liable for a civil penalty not to exceed ten thousand dollars ($10,000) for each violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General or by any district attorney in any court of competent jurisdiction. If brought by the Attorney General, one-half of the penalty collected shall be paid to the treasurer of the county in which the judgment was entered, and one-half to the State Treasurer. If brought by a district attorney, the entire amount of the penalty collected shall be paid to the treasurer of the county in which the judgment was entered.

1798.9. The organization, agency, or individual maintaining an information system or a system of records shall take reasonable precautions to ensure that personal information is accurate, relevant, timely, and complete.

CHAPTER 4. CIVIL REMEDIES

1799. (a) Whenever any organization, agency, or individual fails to comply with any provision of this title in such a way as to have an adverse effect on a data subject, such data subject may bring a civil action against such organization, agency, or individual.

(b) (1) In any suit brought pursuant to the provisions of subdivision (a), relating to refusal of access or refusal to provide a copy of personal information to a data subject, the court may enjoin the organization, agency, or individual from withholding the personal information and order the production to the complainant of any personal information improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the personal information in camera to determine whether such information or any portion thereof may be

ILLUSTRATIVE
LEGISLATION

withheld, and the burden is on the defendant to sustain its action.

(2) The court may assess against the organization, agency, or individual reasonable attorney's fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(c) In any suit brought pursuant to the provisions of subdivision (a) in which the court determines that the defendant acted in a manner which was willful, arbitrary, or capricious, the defendant shall be liable to the complainant in an amount equal to the sum of:

(1) Actual damages sustained by the complainant as a result of such refusal or failure; and

(2) The cost of the action together with reasonable attorney's fees as determined by the court.

(d) An action to enforce any liability created under this section may be brought in any court of competent jurisdiction in the county in which the complainant resides, or has his principal place of business, or in which the defendant's records are situated, within two years from the date on which the cause of action arises, except that where a defendant has materially and willfully misrepresented any information required under this section to be disclosed to a data subject and the information so misrepresented is material to the establishment of the defendant's liability to that data subject under this section, the action may be brought at any time within two years after discovery by the complainant of the misrepresentation.

1799.1. For the purposes of this title, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of such individual.

CHAPTER 5. CRIMINAL PENALTIES

1799.2. (a) Any individual who knowingly and willfully obtains or uses, or attempts to obtain or use, personal information, and who is not authorized to use such information under Section 1798.3 shall be fined not more than five thousand dollars ($5,000) or imprisoned not more than one year, or both.

(b) Any individual, or employee of an individual maintaining a personal information system, who knowingly and willfully provides personal information from the system in violation of this title shall be fined not more than five thousand dollars ($5,000) or imprisoned for not more than one year, or both.

CHAPTER 6. GENERAL EXEMPTIONS

1799.3. (a) The head of any organization or agency may exempt any information system or system of records under its jurisdiction from any part of this title except Section 1798.7, if such system is:

(1) Maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime, or to apprehend criminals, the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of the following:

[i] Information compiled for the purpose of identifying individual criminal offenders or alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status.

[ii] Information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or

[iii] Reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

CHAPTER 7. STATE ARCHIVAL RECORDS

1799.4. (a) Each state agency record which is accepted by the Director of General Services for storage, processing, and servicing in accordance with provisions of the State Administrative Manual shall for the purposes of this section, be considered to be maintained by the state agency which deposited the record and shall be subject to the provisions of this section. The Director of General Services shall not disclose such record, or any information therein, except to the agency responsible for the record or pursuant to rules established by that agency which are not inconsistent with the provisions of this section.

(b) Each state agency record pertaining to an individual which was transferred to the State Archives as a record which has sufficient historical or other value to warrant its continued preservation by the California state government, prior to the effective date of this section, shall for the purposes of this section, be considered to be maintained by the State Archives and shall not be subject to the provisions of this section.

(c) Each state agency record pertaining to an individual which is transferred to the State Archives of the State of California as a record which has sufficient historical or other value to warrant its continued preservation by the California state government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the State Archives and shall be subject to all provisions of this section except subdivision (d) of Section 1798.4 and subdivision (b) of Section 1798.5 and Section 1798.6.

CHAPTER 8. MICELLANEOUS PROVISIONS

1799.5. (a) No provision of this title shall be construed to make confidential any record maintained by the state or any local public entity or private organization which by law is not confidential nor to require disclosure of any record which by law is confidential, or exempt from disclosure, or the disclosure of which is prohibited by law.

(b) No relevant evidence, relating to any procedure established or required by this act shall be privileged in any action for evidentiary purposes including but not limited to discovery procedures or other aspects of any cause of action.

SEC. 2. The Intergovernmental Board on Electronic Data Processing shall study the effects of this title and on April 1, 1977, and April 1, 1978, transmit a report of its findings to a seven-member committee to be composed of the State Director of Finance, the Commissioner of Corporations, the Commissioner of Banking, the Insurance Commissioner, and three other members appointed by the Governor representing the fields of education, health, and criminal justice. This committee shall study the report of the Intergovernmental Board on Electronic Data Processing and transmit that report and the committee's findings and recommendations for further legislation before June 1, 1977, and June 1, 1978.

SEC. 3. The sum of ———— dollars ($————) is hereby appropriated from the General Fund to the State Controller for allocation and disbursement to local agencies pursuant to Section 2231 of the Revenue and Taxation Code to reimburse such agencies for costs incurred by them pursuant to this act.

MICHIGAN

DRAFT #2
SUBSTITUTE FOR

HOUSE BILL NO. 5803

A bill to provide for fair information practices; to create a fair information practices board and prescribe its powers and duties; to create an advisory council on security and privacy of information and prescribe its powers and duties; and to prescribe penalties.

THE PEOPLE OF THE STATE OF MICHIGAN ENACT:

Sec. 1. This act shall be known and may be cited as the "Michigan fair information act".

Sec. 2. As used in this act:

(a) "Access" means a request for or receipt of information, or an attempted access.

(b) "Accurate" means complete, clear, and not ambiguous, to the extent it will not mislead a reasonable person about the true nature or import of the information.

(c) "Agency" means the state or a department, bureau, division, board, commission, authority, state institution of higher education, state court, the legislature, or other entity that is a part of state government, and includes to the extent necessary to carry out this act an entity with which an agency shares use of information.

(d) "Automated" means recorded, in whole or part, on magnetic tape, magnetic disk, magnetic drum, punched card, optically scannable paper or film, or otherwise computer accessible.

(e) "Board means the fair information practices board created in section 7.

(f) "Chief administrative officer" means the administrative head of an agency.

(g) "Correction" means a change in or purge of data and includes supplementation.

(h) "Council" means the advisory council on security and privacy of information.

(j) "Criminal justice agency" means an agency of the state or a political subdivision thereof which performs, as its principal function, activities relating to:

(i) Crime prevention, including research or the sponsorship of research.

(ii) The apprehension, prosecution, adjudication, or rehabilitation of criminal offenders.

(iii) The use of criminal justice record information.

(k) "Criminal justice intelligence information" means background, incident, or investigative information used by a criminal justice agency which is not available to a party in a contested case, but does not include criminal justice record information or information the use of which is specifically prohibited by law.

(l) "Criminal justice record information" means personal information relating to warrants, arrests, pretrial proceedings, convictions, sentencing, rehabilitation and release, or other personal information pertaining to criminal proceedings or generated as a result thereof, but does not include criminal justice intelligence information.

(m) "Data subject" means a person who is the subject of information used by the state.

(n) "Information" or "data" means the normal and computer art meanings of information and of data, whether or not coded, abstracted, personal or nonpersonal, partial or complete, whether public record or not, and regardless of the manner in which it is used.

(o) "Information system" means a process, means, or method designed or used for the collection, production, storage, use, or dissemination of information and includes, without limitation, all manual and computerized systems.

(p) "Person" means an individual, group, association, firm, partnership, trust, corporation, or other legal entity.

(q) "Personal information" means all information describing anything about a person, evidencing things done by or to a person, or otherwise affording a basis from which it is reasonably possible to identify personal characteristics or things done by or to a person.

(r) "Purge" means to cease using, seal, remove, or destroy.

(s) "Sharing" or "sharing of information" means allowing information used by the state to be accessible to a local unit of government, another state, or the federal government or to any person by contract with the state. A fee paid for copies is not a contract with the state for this purpose.

(t) "State" means this state and includes an agency as defined in subdivision (c).

(u) "Timely information" means information recently collected or produced or which, if not recent, remains verifiable, reliable, and pertinent information for the use made of it.

(v) "Use" means collection, production, storage, dissemination, or the normal meaning of use, or an attempted use.

Sec. 3. (1) A person maintaining an automated personal information or data system in this state or concerning residents of this state shall:

(a) Provide reasonable procedures for a data subject to ascertain if a record is kept containing personal information pertaining to the data subject.

(b) Allow a data subject, or in the case of a minor or a person legally incompetent, his next of kin, parent, or guardian, to inspect and obtain at cost, a copy of the information. Copies may be so marked or otherwise made in a manner which will discourage or prevent improper use.

(c) Provide procedures whereby the data subject may challenge the accuracy or timeliness of the information and by which inaccurate or untimely information may be changed and, if change is refused, reasonable opportunity for the data subject to supplement the information.

(d) Advise a person from whom personal information is sought whether the person is legally required to provide the information and, if not, what result may reasonably be expected for failure to provide the information.

(2) A person maintaining an automated personal information or data system subject to this section shall give public notice of the existence and character of its system at least once before January 31 each calendar year. The notice shall be filed with the board. A person maintaining more than 1 system shall file annual notices for each of its systems.

(3) A person who proposes to establish a new automated personal information data system subject to this section shall file a notice with the board within 30 days of establishing the system. The notice shall contain:

(a) The name of the system and the name and address of the person maintaining the system.

(b) The nature and purpose of the system.

(c) The categories and approximate number of persons on whom personal information is expected to be maintained.

(d) Categories of information to be maintained which will be automated.

(e) Policies and practices regarding storage, duration of retention, and disposal of information.

(f) The usual categories of information sources.

(g) The types of use to be made of information.

(h) The description of actions taken to comply with the requirements of subsection (1).

(4) This section applies only to personal information which is automated. This section shall not apply to a person regulated under 15 U.S.C. sections 1681 to 1681t.

(5) The board shall encourage compliance with this section and recommend to the legislature changes in this section or penalties it deems advisable, but shall not have other powers or duties under this section.

(6) Section 20 shall not apply to this section and a criminal penalty shall not be imposed solely for violation of this section.

Sec. 4. Sections 5 to 18 and section 20 apply only to information used by the state.

Sec. 5. (1) The state shall not use personal information unless the information meets each of the following requirements:

(a) It is legally obtained.

(b) There is a valid public purpose for its use.

(c) It is timely.

(d) It is accurate.

(2) The requirement of subsection (1) shall not apply to evidence in a criminal proceeding.

Sec. 6. (1) This act shall govern the use of information by the state, unless otherwise provided herein.

(2) Criminal justice intelligence information is exempt from this act, except that the responsible authority shall require nondisclosure agreements of persons with access to criminal justice intelligence information.

(3) Information used by the state which is not automated and is investigatory information or material compiled or used for regulatory purposes, except to the extent available by law to a party to a contested case, is exempt from this act, except that the responsible authority shall require nondisclosure agreements of persons with access to the information or material.

(4) Information used by a state court or the legislature, exclusively for purposes of internal administration, which is not automated and is not information required to be made available for public inspection by section 21 of Act No. 306 of the Public Acts of 1969, as amended, being section 24.221 of the Michigan Compiled Laws, is exempt from this act.

(5) The board, by rule, may exempt from this act or specified provisions of this act, except section 5, information used by the state which is personnel information concerning a present employee of the agency, is not automated, and is not available to a party in a contested case.

Sec. 7. (1) The fair information practices board is created in the department of management and budget. The powers and duties of the board shall include the power and duty to supervise and implement this act.

(2) The board shall be composed of 8 members. Four members shall be officers or employees of, or otherwise associated with, state government and 4 shall not be associated with state government. A member who is an officer or employee of state government may designate an authorized representative to serve in his place. This right shall be granted by the governor at the time of appointment. Members shall be appointed by the governor with the advice and consent of the senate. The members' terms of office shall be for 4 years, except that of the members first appointed, 4 shall be appointed for 2 years and 4 for 4 years, respectively. On the expiration of a term, a successor shall be appointed. The governor may fill a vacancy for an unexpired term. A member may be removed for cause by the governor. The members shall receive no compensation, but shall be reimbursed for actual and necessary expenses incurred in the performance of their duties in accordance with standard travel regulations issued by the department of management and budget.

(3) The board shall elect 1 of its members as chairman. The term of the chairman shall be 1 year.

(4) The board shall appoint a staff director, who shall be in the classified service, and other personnel authorized by law.

(5) The board shall meet not less than once every 2 months at a time and place in the state determined by the board. The governor, its chairman, or any 3 of its members on 3 days' notice, may call a special meeting at any time or place in the state when deemed necessary. A majority of the membership of the board constitutes a quorum and all decisions of the board shall be by majority vote of those present and voting.

(6) Meetings of the board shall be open to the public, except that after the meeting is called to order, the board may vote to close a meeting, limiting attendance as it deems necessary and appropriate, consistent with the intent of this act. A closing of the meeting shall be by motion made and adopted, with a brief statement of the reason therefor to be made prior to the vote. The brief statement shall be in writing, read aloud by the chairman, and made a part of the record of the meeting.

(7) A record of proceedings containing substantive personal or nonpersonal information may be retained by the board, if necessary, but shall be treated in like manner as if held by the agency which provided it to the board.

(8) Records not required by law to be made available for public inspection are considered specifically exempt from public inspection for purposes of this section.

Sec. 8. (1) The powers and duties of the board shall be broadly construed to allow full implementation of the purpose and intent of this act. The powers and duties of the board include the following:

(a) To review and decide appeals of persons relative to rights and duties under this act.

(b) To supervise and enforce this act relating to the use of information by the state.

(c) To conduct inquiries and investigations appropriate to carry out its functions.

(d) To have access to information used by the state for each of its members and its staff as it deems appropriate.

(e) To make recommendations concerning fair information practices and to report periodically to the governor, legislature, and judiciary.

(f) To receive and act on the advice of the advisory council on security and privacy of information.

(2) The board may promulgate rules under this act to implement its powers and duties, pursuant to Act No. 306 of the Public Acts of 1969, as amended, being sections 24.201 to 24.315 of the Michigan Compiled Laws. Rules of the board may:

(a) Establish requirements and procedures adequate to assure that information subject to this act is legally obtained, serves a valid public purpose, and is timely and accurate.

(b) Require adequate security for information and information systems, including nondisclosure agreements when the board deems them necessary or advisable.

(c) Determine criteria and procedures relative to orders to change information and as to sealing, removing and destroying information, whether by agency action or order of the board.

(d) Set forth procedures for and limitations on use on a need to know basis.

(e) Establish procedures for notice, access, review, change of information, and appeal, consistent with this act.

(f) Establish procedures for and controls and limitations on the use of information for research and for the sharing of information, which may include the prohibition thereof, if necessary to carry out the intent of this act.

(g) Provide a data access control plan or manual, or both, and education programs relative to proper security and privacy practices required by this act and rules promulgated under it.

(h) Require adequate record keeping of use of information including, to the extent deemed necessary by the board, records as to the source of information.

Sec. 9. (1) An advisory council on security and privacy of information, consisting of 11 members to be ap-

pointed by the governor with the advice and consent of the senate, is created under the board.

(2) The council shall conduct continuing study and review and make recommendations to the board on questions of individual privacy, confidentiality, and system security relevant to the collection, production, storage, usage, and dissemination of information by the state and shall be the chief advisory body to the board on matters relating to security and privacy.

(3) A majority of members shall not be in government service. The terms of the members shall be for 4 years, except that of the members first appointed, 5 shall be appointed for 2 years, and 6 for 4 years. On the expiration of a term a successor shall be appointed. The governor may fill a vacancy for an unexpired term. A member may be removed for cause by the governor. The members shall not receive compensation, but shall be reimbursed for actual and necessary expenses incurred in the performance of their duties in accordance with standard travel regulations issued by the department of management and budget.

(4) The council shall elect 1 of its members as chairman. The term of chairman shall be 1 year. The council shall meet at the call of its chairman, or any 4 of its members of 3 days' notice, to carry out its responsibilities under this act. The board shall assist the council in the collection and analysis of information.

(5) The council shall appoint a person to the position of security and privacy ombudsman, who shall be in the classified service, and other personnel authorized by law. The ombudsman shall act as liaison to the board, may represent persons before the board, and shall be the staff director for the council.

Sec. 10. A public register of types of information collected, produced, stored, used, or disseminated, shall be maintained by the state at each place where a data subject may have access. The register shall set forth, with respect to each agency using information:

(a) The name and location of the agency.

(b) The custodian of the information.

(c) The types of information.

(d) The general purpose for and use of the information.

(e) Whether or not a person must provide the information and normal consequences of failure to provide it.

Sec. 11. A person other than the data subject having use of or access to information used by the state shall not:

(a) Submit to or permit unauthorized use of the information.

(b) Seek to benefit personally or permit others to benefit personally by information which has come to him as a result of work assignment.

(c) Remove information or cause it to be removed from a file or system without authorization.

(d) Operate or request or permit others to operate equipment utilized in the use of information without authorization.

(e) Violate a nondisclosure agreement.

(f) Fail to comply with a valid order of the board.

(g) Otherwise fail to comply with this act or rules promulgated hereunder.

Sec. 12. (1) The chief administrative officer of an agency which uses information subject to this act is the custodian of that information. A request for access shall be made to the custodian or his authorized representative.

(2) Within the provisions of this act a data subject has a right of access to information of which he is the subject. Access shall include the right to view, take notes, and receive copies, if feasible.

(3) An agency may prescribe reasonable hours, manners, and places for access, and, at the allowance or direction of the board, shall impose restrictions reasonably necessary to assure the security and privacy of the information and to verify the identity of the person who seeks access to the information. The board shall establish conditions for and limitations on the use of fingerprinting for verification of identity of the person.

(4) A person who is the subject of information used by the state and who believes the information is being used in violation of section 5 may make sworn application to the agency having custody or control of the information, in writing, to correct the information. The application shall include identification as required and the basis for the requested correction. If the agency declines or fails to act, as requested, within 30 days after the application is made, or the person believes a decision or action of the agency to be unsatisfactory, he shall have the right to appeal, as set forth in section 15.

(5) An agency shall not charge more than its cost for copies made and provided under this section unless otherwise provided by law.

Sec. 13. (1) Access by a data subject includes the right to have an attorney or other person present with him or represent him.

(2) A minor or a person legally incompetent may be denied access to records other than public records if provision is made for access by a next of kin, parent, guardian, professional, or attorney authorized by a next of kin, parent, or guardian. The board, by rule, may provide for similar denial of access by persons to health and mental health records pertaining to diagnosis, treatment, or prognosis.

(3) The board, by rule or on a case by case basis, may approve access by other than normally authorized personnel, a data subject or a person specified in this section if the board determines the access desirable to carry out this act. Conditions, procedures, controls, and limitations may be set by the board, including requiring execution of nondisclosure agreements.

Sec. 14. An agency, or combinations thereof, may designate a person or group to review requests by a data subject for access or change of information. A person aggrieved by a decision of the reviewing person or group may appeal to the board as provided in section 15.

Sec. 15. (1) Appeals from actions by an agency of the state relating to the performance of its duties under this act shall be to the board. The appeal shall be in writing, sworn to, and shall specify the agency and information in question, the date of application to the agency and known disposition thereof, the basis for the appeal, and the action requested of the board. The board may reject a frivolous appeal without hearing.

(2) Except as provided in subsection (1), the board shall order the requested change without a hearing, stipulate in writing with the applicant to an order based on a modified request, or conduct a hearing at which the person appealing may appear with or without counsel, present evidence, and examine and cross-examine witnesses. Procedures shall be determined by rules promulgated by the board consistent with Act No. 306 of the Public Acts of 1969, as amended, for hearings in contested cases. The board may appoint 1 or more of its members or employees to conduct an appeal hearing. Written findings of fact and conclusions of law and a pertinent order shall be issued by the board within 90 days after receipt of an appeal, excluding extensions requested by the applicant. On proof of a right to correction, the board shall order the information appropriately corrected. Notification of an ordered correction shall be disseminated by the board to agencies using the information in question and to the person whose information has been ordered corrected.

Sec. 16. (1) The board may conduct an investigation to determine whether a person has violated or is about to violate sections 5 to 18 of this act or a rule promulgated thereunder.

(2) If the board finds that this act or a rule was violated, the board may, after notice of at least 4 days by personal service or certified mail, hold a hearing to determine whether a cease and desist order should issue to restrain the action or practice which is in violation of this act or the rule. The board may designate 1 or more of its members or employees to conduct the hearings.

(3) For the purpose of an investigation under this act, the board or a member thereof designated by rule of the board, may administer oaths or affirmations, and on its own motion or on request of a party may subpoena witnesses, compel their attendance, take evidence, and require the production of matter which is relevant to the investigation, including the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things, and the identity and location of persons having knowledge of relevant facts, or any other matter reasonably calculated to lead to the discovery of material evidence.

(4) Upon failure to obey a subpoena or to answer questions propounded by the investigating officer and upon reasonable notice to all persons affected thereby, the board may apply to the circuit court of the county in which the investigation is being conducted or the proceeding is being conducted, for an order compelling compliance.

(5) All proceedings under this section shall be in accordance with Act No. 306 of the Public Acts of 1969, as amended.

(6) After notice and hearing, the board may order a person it finds to be in violation to cease and desist.

Sec. 17. A person aggrieved by a final order of the board may appeal the order to the circuit court in accordance with general court rules and sections 101 to 106 of Act No. 306 of the Public Acts of 1969, as amended.

Sec. 18. (1) On or after July 1, 1976, a request for public record information from the state in order to be allowed to obtain a copy of the information shall be by name or other personal identifier, unless otherwise approved by the board.

(2) On or after July 1, 1976, information shall not be disseminated at a discount cost or charge for volume, nor in computer-accessible form, nor by blanket order, subscription, or similar continuing agreement, unless approved by the board.

(3) The board, by rule, consistent with section 21 of Act No. 306 of the Public Acts of 1969, as amended, may provide that access to personal information used by the state, whether or not deemed a public record, may be restricted as the board deems necessary and proper to restrict or prevent use, by other than the person who is the subject of the information, contrary to the intent of this act.

(4) This section does not apply to use by authorized personnel in carrying out their duties for the state.

Sec. 19. (1) A person may institute a civil action for damages or to restrain a violation of this act. In an action for damages, a person who wilfully violates this act shall be liable, in addition to any liability for actual damages as may be proven, for exemplary damages as may be determined by the court for each wilful violation, together with costs and reasonable attorney's fees incurred by the person bringing the action.

(2) A person shall not be subject to civil or criminal liability under this act for denial of access to another person if the denial is made because the demand is reasonably believed to be part of a pattern of clearly unreasonable, repetitive demands for access by or on behalf of the other person.

Sec. 20. (1) The wilful violation of a provision of this act, except as provided in section 3, shall be a misdemeanor punishable by imprisonment for not more than 1 year, or a fine of not more than $10,000.00, or both.

(2) The violation of a rule promulgated under this act shall be a disdemeanor punishable by a fine of not more than $500.00.

Sec. 21. This act shall be construed in a manner consistent with the freedom of information provisions of Act No. 306 of the Public Acts of 1969, as amended.

Sec. 22. A person shall not have a defense of sovereign immunity against an action brought for violation or threatened violation of this act.

Sec. 23. This act shall become effective July 1, 1975.

MINNESOTA STATUTE

FIRST REGULAR SESSION

OFFICIAL RECORDS—COLLECTION, SECURITY AND DISSEMINATION

CHAPTER 401
H.F.No.1014

An Act relating to the collection, security and dissemination of data on individuals by the state and its political subdivisions; clarifying necessary definitions; changing reporting requirements; restructuring the duties of responsible authorities and the rights of subjects of data; providing for issuance of rules relating to the implementation of the act by the commissioner of administration; providing for the establishment of a privacy study commission; providing penalties; appropriating money; amending Minnesota Statutes 1974, Sections 15.162; 15.163; 15.165; 15.166; 15.167; and Chapter 15, by adding sections; repealing Minnesota Statutes 1974, Sections 15.164 and 15.168.

Be it enacted by the Legislature of the State of Minnesota:

Section 1. Minnesota Statutes 1974, Section 15.162, is amended to read:

15.162 Collection, security and dissemination of records; definitions

Subdivision 1. As used in sections 15.162 to 15.168 the terms defined in this section have the meanings given them.

Subd. 2. "Commissioner" means the commissioner of the department of administration.

Subd. 2a. "Confidential data on individuals" means data which is not public but is (a) expressly made confidential by law as to the individual subject of that data; (b) collected by a civil or criminal investigative agency as part of an active investigation undertaken for the purpose of the commencement of a legal action, provided that the burden of proof as to whether such investigation is active or in anticipation of a legal action is upon the agency; (c) data which supplies the basis for the diagnosis of the medical or psychiatric condition of an individual as determined by a licensed physician.

Subd. 3. "Data on individuals" includes all records, files and processes which contain any data in which an individual is or can be identified and which is kept or intended to be kept on a permanent or temporary basis. It includes that collected, stored, and disseminated by manual, mechanical, electronic or any other means. Data on individuals includes data classified as public, private or confidential.

Subd. 4. "Individual" means a natural person. In the case of a minor individual under the age of 18, "individual" shall mean a parent or guardian acting in a representative capacity, except where such minor individual indicates otherwise.

Subd. 5. "Political subdivision" includes counties, municipalities, school districts and any boards, commissions, districts or authorities created pursuant to local ordinance. It includes any nonprofit corporation which is a community action agency organized to qualify for public funds, or any non-profit social service agency which performs services under contract to any political subdivision, statewide system or state agency.

Subd. 5a. "Private data on individuals" means data which is not public but which by law is accessible to the individual subject of that data.

Subd. 5b. "Public data on individuals" means data which is accessible to the public in accordance with the provisions of section 15.17.

Subd. 6. "Responsible authority" at the state level means any office established by law as the body responsible for the collection and use of any set of data on individuals or summary data. "Responsible authority" in any political subdivision means the person designated by the governing board of that political subdivision, unless otherwise provided by state law. With respect to statewide systems, "responsible authority" means the state official involved, or if more than one state official, the official designated by the commissioner.

Subd. 7. "State agency" means the state, the university of Minnesota, and any office, officer, department, division, bureau, board, commission, authority, district or agency of the state.

Subd. 8. "Statewide system" includes any record-keeping system in which data on individuals is collected, stored, disseminated and used by means of a system common to one or more agencies of the state or more than one of its political subdivisions.

Subd. 9. "Summary data" means statistical records and reports derived from data on individuals but in which individuals are not identified and from which neither their identities nor any other characteristic that could uniquely identify an individual is ascertainable.

Sec. 2. Minnesota Statutes 1974, Section 15.163, is amended to read:

15.163 Reports to the legislature

Subdivision 1. On or before August 1 of each year the responsible authority shall document and file a report with the commissioner of administration, which shall be a public record. The report shall contain the following information:

(a) The title, name, and address, of the responsible authority.

(b) A statement of which records containing data on individuals maintained by the responsible authority are classified as confidential and which are classified as private. The responsible authority shall submit sample copies of any forms which will, when executed, contain data on individuals classified as private or confidential.

(c) The purposes for which private or confidential data on individuals is authorized to be used, collected, disseminated and stored.

(d) The responsible authority's policies and practices regarding storage, duration of retention, and disposal of data on individuals, including a description of the provisions for maintaining the integrity of private and confidental data on individuals.

Subd. 2. On or before December 1 of each year, the commissioner shall prepare a report to the legislature summarizing the information filed by responsible authorities pursuant to subdivision 1 and notifying the legislature of any problems relating to the administration, implementation and enforcement of sections 15.162 to 15.168 which might, in his opinion, require legislative action.

Sec. 3. Minnesota Statutes 1974, Chapter 15, is amended by adding a section to read:

15.1641 Duties of responsible authority

(a) Data on individuals is under the jurisdiction of the responsible authority who may appoint an individual to be in charge of each file or system containing data on individuals.

(b) Collection and storage of public, private or confidential data on individuals and use and dissemination of private and confidential data on individuals shall be limited to that necessary for the administration and management of programs specifically authorized by the legislature, local governing body or mandated by the federal government.

(c) Private or confidential data on individuals shall not be used, collected, stored or disseminated for any purposes other than those stated to an individual at the time of collection in accordance with section 15.165 or, in the case of data collected prior to August 1, 1975, for any purpose other than those originally authorized by law, unless (1) the responsible authority files a statement with the commissioner describing the purpose and necessity of the purpose with regard to the health, safety or welfare of the public and the purpose is approved by the commissioner, or (2) the purpose is subsequently authorized by the state or federal legislature, or (3) the purpose is one to which the individual subject or subjects of the data have given their informed consent.

(d) The use of summary data derived from private or confidential data on individuals under jurisdiction of one or more responsible authorities shall be permitted, provided that summary data is public pursuant to section 15.17. The responsible authority shall prepare summary data from private or confidential data on individuals upon the request of any person, provided that the request is in writing and the cost of preparing the data is borne by the requesting person. The responsible authority may delegate the power to prepare summary data to the administrative officer responsible for any central repository of summary data, or to a person outside of its agency if the person agrees in writing not to disclose private or confidential data on individuals.

(e) The responsible authority shall establish procedures and safeguards to ensure that all public, private or confidential data on individuals is accurate, complete and current. Emphasis shall be placed on the data security requirements of computerized files containing private or confidential data on individuals which are accessible directly via telecommunications technology, including security during transmission.

Sec. 4. Minnesota Statutes 1974, Section 15.165, is amended to read:

15.165 Rights of subjects of data

The rights of individuals on whom the data is stored or to be stored shall be as follows:

(a) An individual asked to supply private or confidential data concerning himself shall be informed of: (1) both the purpose and intended use of the requested data, (2) whether he may refuse or is legally required to supply the requested data, and (3) any known consequence arising from his supplying or refusing to supply private or confidential data.

(b) Upon request to a responsible authority, an individual shall be informed whether he is the subject of stored data on individuals, whether it be classified as public, private or confidential. Upon his further request, an individual who is the subject of stored public or private data on individuals shall be shown the data without any charge to him and, if he desires, informed of the content and meaning of that data. After an individual has been shown the data and informed of its meaning, the data

need not be disclosed to him for six months thereafter unless a dispute or action pursuant to this section is pending or additional data on the individual has been collected. The responsible authority shall provide copies of the data upon request by the individual subject of the data, provided that the cost of providing copies is borne by the requesting individual.

(c) An individual may contest the accuracy or completeness of public or private data concerning himself. To exercise this right, an individual shall notify in writing the responsble authority describing the nature of the disagreement. The responsible authority shall within 30 days correct the data if the data is found to be inaccurate or incomplete and attempt to notify past recipients of inaccurate or incomplete data, or notify the individual of disagreement. Data in dispute shall not be disclosed except under conditions of demonstrated need and then only if the individual's statement of disagreement is included with the disclosed data. The determination of the responsible authority is appealable in accordance with the provisions of the administrative procedure act[1] relating to contested cases.

Sec. 5. Minnesota Statutes 1974, Section 15.166, is amended to read:

15.166 Civil penalties

Subdivision 1. Notwithstanding section 466.03, a political subdivision, responsible authority or state agency which violates any provision of sections 15.162 to 15.168 is liable to a person who suffers any damage as a result of the violation, and the person damaged may bring an action against the political subdivision, responsible authority or state agency to cover any damages sustained, plus costs and reasonable attorney fees. In the case of a willful violation, the political subdivision or state agency shall, in addition, be liable to exemplary damages of not less than $100, nor more than $1,000 for each violation. The state is deemed to have waived any immunity to a cause of action brought under sections 15.162 to 15.168.

Subd. 2. A political subdivision, responsible authority or state agency which violates or proposes to violate sections 15.162 to 15.168 may be enjoined by the district court. The court may make any order or judgment as may be necessary to prevent the use or employment by any person of any practices which violate sections 15.162 to 15.168.

Subd. 3. An action filed pursuant to this section may be commenced in the county in which the individual alleging damage or seeking relief resides, or in the county wherein the political subdivision exists, or in the case of the state, any county.

Sec. 6. Minnesota Statutes 1974, Section 15.167, is amended to read:

[1] Section 15.0424 et seq.

15.167 Penalties

Any person who willfully violates the provisions of sections 15.162 to 15.168 or any lawful rules and regulations promulgated thereunder is guilty of a misdemeanor. Willful violation of sections 15.162 to 15.168 by any public employee constitutes just cause for suspension without pay or dismissal of the public employee.

Sec. 7. Minnesota Statutes 1974, Chapter 15, is amended by adding a section to read:

15.1671 Duties of the commissioner

The commissioner shall with the advice of the intergovernmental information services advisory council promulgate rules, in accordance with the rule-making procedures in the administrative procedures act which shall apply to state agencies, statewide systems and political subdivisions to implement the enforcement and administration of sections 15.162 to 15.169. The rules shall not affect section 15.165, relating to rights of subjects of data, and section 15.169, relating to the powers and duties of the privacy study commission. Prior to the adoption of rules authorized by this section the commissioner shall give notice to all state agencies and political subdivisions in the same manner and in addition to other parties as required by section 15.0412, subdivision 3, of the date and place of hearing, enclosing a copy of the rules and regulations to be adopted.

Sec. 8. Minnesota Statutes 1974, Chapter 15, is amended by adding a section to read:

15.169 Privacy study commission

Subdivision 1. Establishment. There is hereby created a privacy study commission consisting of six members, three of whom shall be appointed by the committee on committees, and three of whom shall be appointed by the speaker of the house. The commission shall act from the time its members are appointed until the commencement of the 1977 regular session of the legislature. Any vacancy shall be filled by the appointing power.

Subd. 2. Organization and procedure. At its first meeting the commission shall elect a chairman, a vice-chairman and such other officers from its membership as it may deem necessary. The commission shall adopt rules governing its operation and the conduct of its meetings and hearings, which rules are not subject to the provisions of the administrative procedures act.

Subd. 3. Duties and powers. The commission shall make a continuing study and investigation of data on individuals collected, stored, used and disseminated by political subdivisions, state agencies, statewide systems and any other public or private entity in the state of Minnesota the commission may deem appropriate for such study and investigation. The powers and duties of the commission shall include, but are not limited to the following:

(1) the holding of meetings at times and places it designates to accomplish the purposes set forth in Laws 1975, Chapter 401. The commission may hold hearings at times and places convenient for the purpose of taking evidence and testimony to effectuate the purposes of Laws 1975, Chapter 401, and for those purposes the commission may, through its chairman by a three-fourths vote of its members, issue subpoenas, including subpoenas duces tecum, requiring the appearance of persons, production of relevant records and the giving of relevant testimony. In the case of contumacy or refusal to obey a subpoena issued under authority herein provided, the district court in the county where the refusal or contumacy occurred may, upon complaint of the commission, punish as for contempt the person guilty thereof.

(2) the study of all data on individuals collected, stored, used or disseminated in the state of Minnesota including, but not limited to that collected, stored, used or disseminated by any political subdivision, state agency or statewide system in order to determine the standards and procedures in force for the protection of private and confidential data on individuals. In conducting such study, the commission shall:

(a) determine what executive orders, attorney general opinions, regulations, laws or judicial decisions govern the activities under study and the extent to which they are consistent with the rights of public access to data or individuals, privacy, due process of law and other guarantees in the Constitution.

(b) determine to what extent the collection, storage, use or dissemination of data on individuals is affected by the requirements of federal law.

(c) examine the standards and criteria governing programs, policies and practices relating to the collection, storage, use or dissemination of data on individuals in the state of Minnesota.

(d) collect and utilize to the maximum extent practicable, all findings, reports, studies, hearing transcripts, and recommendations of governmental legislature, and private bodies, institutions, organizations and individuals which pertain to the problems under study by the commission.

(3) the recommendation to the legislature of the extent, if any, to which the requirements and principles of this act should be applied to information practices in existence in the state of Minnesota by legislation, administrative action or voluntary adoption of such requirements and principles, and report on such other legislative recommendations as it may determine to be necessary to protect the privacy of individuals while meeting the legitimate needs of government and society for information.

Subd. 4. Office. The commission shall maintain an office in the capitol group of buildings in space provided by the commissioner of administration.

Subd. 5. Supplies; staff. The commission may purchase equipment and supplies and employ such professional, clerical, and technical assistants from the senate and house staff as it deems necessary in order to perform the duties herein prescribed. The commission may invite consultants and other knowledgeable persons to appear before it and offer testimony and compensate them appropriately.

Subd. 6. Assistance of other agencies. The commission may request any information including any data on individuals from any political subdivision, statewide system, or state agency or any employee thereof in order to assist in carrying out the purposes of the act, and notwithstanding any law to the contrary, such employee or agency is authorized and directed to promptly furnish any such data or information requested.

Subd. 7. Expense, reimbursement. Members of the commission shall be compensated as provided in Minnesota Statutes, Section 3.102.

Subd. 8. Penalties for disclosure. (1) Any member, assistant or staff of the commission who, by virtue of his employment or official position, has possession of, or access to, agency records which contain private or confidential data on individuals the disclosure of which is prohibited by law, and also knowing or having reason to know that disclosure of such data is prohibited, willfully discloses such data in any manner to any person or agency not entitled to receive it shall be guilty of a misdemeanor.

(2) Any member, assistant or staff of the commission who knowingly and willfully requests or obtains any private or confidential data on individuals under false pretenses the disclosure of which such person is not entitled by law shall be guilty of a misdemeanor.

Subd. 9. Report to the legislature. The commission shall report its findings and recommendations to the legislature as soon as they are available, in any case not later than November 15, 1976, and may supplement them thereafter until January 15, 1977. One copy of the report shall be filed with the secretary of the senate, one copy with the chief clerk of the house of representativs and ten copies with the legislative reference library.

Subd. 10. Appropriation. There is appropriated from the general fund the sum of $25,000 for the biennium ending June 30, 1977, or as much thereof as necessary, to pay the expenses incurred by the commission. Expenses of the commission shall be approved by the chairman or another member as the rules of the commission provide and paid in the same manner that other state expenses are paid.

Sec. 9. Minnesota Statutes 1974, Sections 15.164 and 15.168, are repealed.

Sec. 10. This act is effective the day following final enactment.

Approved June 5, 1975.

NATIONAL ASSOCIATION OF STATE
INFORMATION SYSTEMS

SUGGESTED GUIDELINES FOR

A STATE INFORMATION PRACTICES ACT

An Act to protect a person's right to privacy and confidentiality and to prohibit the unreasonable acquisition, use and retention of such information by state and local governments.

(Enactment Clause, as required by state law)

SECTION 1. Short Title. This Act shall be known and may be cited as the "Information Practices Act".

SECTION 2. Legislative Intent.

(a) The (name of legislative body) finds and declares:

(i) That the use of information for purposes other than those purposes to which a person knowingly consents can seriously endanger a person's right to privacy and confidentiality.

(ii) That information collection methods are not limited to political boundaries and, therefore, it is necessary to establish a unified statewide program for the regulation of information collection practices and to cooperate fully with other states and with agencies of the government of the United States in regulating such information collection practices.

(iii) That in order to increase participation of persons in the prevention and correction of unfair information practices, opportunity for hearing and remedies must be provided.

(iv) That in order to insure that information collected, stored and disseminated about persons is consistent with fair information practices while safe-guarding the interests of the persons and allowing the state to exercise its proper powers, a definition of rights and responsibilities must be established.

(b) It is the purpose of this act to establish fair information practices to insure that the rights of persons are protected and that proper remedies are established to prevent abuse of personal information.

SECTION 3. Definitions. As used by this act, unless the context otherwise requires, the following words and phrases shall have the meaning ascribed to them in this section;

(a) "Act" is the (name of state) Information Practices Act.

(b) "Board" is the (name of state) Information Practices Board created by this act (or if there is no board as in Option 5 infra, (b) shall read "Authority" is the (name of state) Information Practices Authority created by this Act.

(c) "Individual" is any man, woman, or child.

(d) "Person" is any individual, partnership, co-partnership, firm, company, corporation, association, joint stock company, trust, estate, political subdivision, state agency, or any other legal entity, or their legal representatives or agent.

(e) "Personal information" is any information that by some specific means of identification, including but not limited to any name, number, description, and including any combination of such characters, it is possible to identify with reasonable certainty the *person* to whom such information pertains.

(f) "Personal information system" is any method by which personal information is collected, stored, or disseminated by any agency of this state government, or, by any local government or other political subdivision of this State.

(g) "Responsible authority" at the State level means any office established by law as the body responsible for the collection and use of any set of data on persons or summary data. "Responsible authority" in any political subdivision means the person designated by the governing body (authority) of that political subdivision, unless otherwise provided by state law. With respect to statewide systems, those involving one or more state agencies and one or more political subdivisions, "responsible authority" means the state official involved, or if more than one state official, the state official designated by the board.

(h) "File" is the point of collection of personal identifiable information.

(i) "Purge" is the physical destruction of files, records, or information.

(j) "Need to know" is the necessity of the person who wishes to collect, store, or disseminate personal information for obtaining the specific information.

(k) "Local government" (the appropriate definition for the purposes of this act in this state).

(l) "Political subdivision" (appropriate definition for the purposes of this act in this state).

(m) "Machine-accessible" means recorded on magnetic tape, magnetic disk, magnetic drum, punched card, optically scannable paper or film, punched paper tape, or any other medium by means of which information can be communciated to data processing machines.

SECTION 4. (Name of state) Information Practices Board.

(Option 1 — Independent Board):

(a) There is established in the executive branch of this state government an agency to be known as Information Practices Board. The Board shall be composed of nine persons who shall be appointed by the Governor with the advice and consent of (name of legislative body charged with confirmation of Governor's appointments). One such person shall have been actively engaged in the management of information and record keeping systems in this State government, one such person shall have been actively engaged in information processing and record keeping systems in local government in this state, one such person shall have been actively engaged in information processing and record keeping systems in criminal justice or law enforcement, and six of such persons, at least 2 of whom shall represent the general public, shall not be representative of any of the aforementioned activities. Initially, three of such persons shall be appointed to serve until (term desired for staggering); three of such persons shall be appointed to serve until (term desired for staggering); and three of such persons shall be appointed to serve until (term desired for staggering). As terms of appointment expire, successors shall be appointed for terms to expire (desired length of term) years thereafter except all members of the Board shall serve until their respective successors are appointed and qualified. The Governor shall fill any vacancy by the appointment of a member for the unexpired term of such member in the same manner as in the making of original appointments.

(b) The Board may appoint a Director who shall serve at the pleasure of the Board, and such other employees as are necessary to carry out the purposes of this act. The Board may secure by agreement such services as it may deem necessary from any other department agency or unit of state government, and may employ and compensate whatever consultants and technical assistants may be required. It is the policy of the legislature that the Board shall use existing state capability insofar as practicable.

(c) The Board shall meet at least once every three months, and each member of the Board shall be entitled to reimbursement for actual and necessary expenses incurred in the performance of his duties.

(Option 2—Board within Existing State Department):

(a) There is established within the Department of Administration (or other appropriate state agency) an Information Practices Board.

Board shall be composed of nine persons who shall be appointed by the Governor with the advice and consent of (name of legislative body charged with confirmation of Governor's appointments). One such person shall have been actively engaged in the management of information and record keeping systems in this State government, one such person shall have been actively engaged in information processing and record keeping systems in local government in this state, one such person shall have been actively engaged in information processing and record keeping systems in criminal justice or law enforcement, and six of such persons, at least 2 of whom shall represent the general public, shall not be representative of any of the aforementioned activities. Initially, three of such persons shall be appointed to serve until (term desired for staggering); and three of such persons shall be appointed to serve until (term desired for staggering). As terms of appointment expire, successors shall be appointed for terms to expire (desired length of term) years thereafter except all members of the Board shall serve until their respective successors are appointed and qualified. The Governor shall fill any vacancy by the appointment of a member for the unexpired term of such member in the same manner as in the making of original appointments.

(b) The Board may appoint a Director who shall be an official of the Department of Administration (or other appropriate state agency). The Board may secure from the Department of Administration (or other appropriate agency) such services as it may deem necessary.

(c) The Board shall meet at least once every three months, and each member of the Board shall be entitled to reimbursement for actual and necessary expenses incurred in the performance of his duties.

(Option 3 — Ex Officio Board)

(a) There is established an Information Practices Board. The Board shall be composed of (e.g., the Governor, the Attorney General, the Chief Justice of the Supreme Court, the President of the Senate, the Speaker of the House, or their designees) serving ex officio.

(b) The Board may appoint a Director who shall be an official of the Department of Administration (or other appropriate state agency). The Board may secure from the Department of Administration (or other appropriate agency) such services as it may deem necessary.

(c) The Board shall meet at least once every three months, and each member of the Board shall be entitled to reimbursement for actual and necessary expenses incurred in the performance of his duties.

(Option 4 — No Board):

(a) There is established an Information Practices Authority which shall be the Director of the Department of Administration (or other appropriate state official) serving ex officio.

(b) Intentionally deleted.

(c) Intentionally deleted.

End of Options

(d) The Board (Authority) shall collect and disseminate such information and acquire such technical data as may be required to carry out the purposes of this Act, including ascertainment of the routine practices and security procedures of personal information systems in the collection, storage or dissemination of personal information.

(e) The Board (Authority) may require the submission of complete outlines or plans of personal information systems from responsible authorities and the submission of such reports regarding known or alleged violations of the Act or of regulations thereunder, as may be necessary for purposes of this act.

(f) The Board (Authority) shall prescribe a program of continuing and regular inspection of personal informa-

tion systems in order to assure that information practices are in compliance with this Act and regulations adopted thereunder.

(g) The Board (Authority) shall investigate alleged violations of this Act or of regulations adopted thereunder.

(h) The Board (Authority), pursuant to procedures (of this Act or Administrative Procedures Act), shall adopt regulations to promote security, confidentially and privacy in personal information systems, consistent with the purpose of this Act. Without limiting the generality of this authority, such regulation shall prescribe:

(1) limits of authority and responsibility for all persons with access to personal information systems or any part thereof;

(2) methods for obtaining advice and opinions with regard to requirements of law in the regulating of security, confidentiality and privacy in personal information systems;

(3) policies and procedures to insure the security of personal information systems including the mechanics, personnel, processing of information, site design and access.

(4) standards, over and above those required by normal civil service, of conduct, employment and discipline for responsible authorities and all other persons with access to personal information systems or any part thereof;

(5) standards for the need to know to be utilized by responsible authorities in determining what types of information may be collected, stored and disseminated;

(6) standards for direct and indirect access to personal information systems;

(7) standards and procedures to assure the prompt and complete purging of personal information from personal information systems;

(8) a continuing program of external and internal auditing and verification to assure the accuracy and completeness of personal information;

(9) standards governing interagency use of files as long as such use is not in violation of other statutory requirements, this Act or regulations adopted thereunder.

(10) standards for exempting certain files from the coverage of this act such as telephone number lists, mailing lists, etc. intended for normal office use.

(i) The Board (Authority) shall have the duty to represent the State of (name of state) in any and all matters pertaining to plans, procedures or negotiations for interstate compacts or other governmental arrangements relating to the regulations of personal information systems or otherwise relating to the protection of the person's right of privacy.

(j) The Board (Authority) shall have the authority to accept, receive and administer on behalf of the State any grants, gifts, loans or other funds made available to the State from any source for purposes of this Act or other related privacy protection activities, surveys or programs, subject to the several statutes and procedures of (name of state).

(k) On or before December 1 (or other desired date) of each year the Board shall prepare a report, or update of the previous year's report, to the legislature and governor. Summaries of the report be available to the public at a nominal cost. The report shall contain to the extent feasible at least the following information:

(1) a complete listing of all personal information systems which are kept by the state and its political subdivisions, a description of the information contained therein, and the reason that the information is kept;

(2) a statement of which types of personal information in the Board's opinion, are public records as defined by (name of state) Statutes, which types of information are confidential and which types of information are neither;

(3) the title, name, and address of the responsible authority for the system and for each file and associated procedures;

(i) the categories and number of persons in each category on whom information is or is expected to be maintained,

(ii) the categories of information maintained, or to be maintained, indicating which categories are or will be stored in machine-accessible files.

(iii) the categories of information sources,

(iv) a description of all types of use made of information, indicating those involving machine-accessible files. and including all classes of users,

(v) the responsible authority's and the Board's policies and practices regarding information storage, duration of retention of information, and disposal thereof,

(vi) a description of the provisions for maintaining the integrity of the information pursuant to this Act and the regulations adopted thereunder, and

(vii) the procedures pursuant to this Act and the regulations adopted thereunder whereby a person can (a) be informed if he is the subject of information in the system, (b) gain access to the information, and (c) contest its accuracy, completeness, pertinence, and the necessity for retaining it; and

(4) any recommendations concerning appropriate legislation.

(Section (1) and (m) are not required if the state has an Administrative Procedures Act.)

(1) The Board (Authority) may adopt such procedural rules as may be necessary to accomplish the purposes of this Act. Notice of the proposed adoption of procedural rules shall be given in accord with subsection (m) of this section 4, and any person may submit written statements regarding such proposals.

(m) The Board (Authority) shall consider written proposals for the adoption, amendment or repeal of Board (Authority) regulations presented by any person, and the Board (Authority) may make such proposals on its own motion. If the Board (Authority) finds that any such proposal is supported by an adequate statement of reasons, is accompanied by a petition signed by at least 500 persons, is not plainly devoid of merit and does not deal with a subject on which a hearing has been held within the preceding six months, the Board shall schedule a public hearing for consideration of the proposal. If such proposal is made at the Board's (Authority's) discretion, the Board (Authority) shall schedule a public hearing without regard to the above conditions.

No substitute regulations shall be adopted, amended or repealed until after a public hearing has been held within the State. At least 20 days prior to the scheduled date of the hearing the Board (Authority) shall give notice of such hearing by public advertisement in three newspapers of general circulation in the State of the date, time, place, and purpose of such hearing; give written notice to any person in the State concerned who has in writing requested notice of public hearings; and make available to any person on request copies of the proposed regulations, together with summaries of the reasons supporting their adoption.

Any public hearing relating to the adoption, amendment, or repeal of Board (Authority) regulations under this subsection shall be held before a qualified Hearing Officer appointed by the Board (Authority). All such hearings shall be open to the public, and reasonable opportunity to be heard with respect to the subject of the hearing shall be recorded stenographically. The transcript so recorded, and any written submissions to the Hearing Officer in relation to such hearings shall be open to public inspection, and copies thereof shall be made available to any person upon payment of the actual cost of reproduction of the original.

After such hearing, the Hearing Officer shall make recommendations to the Board (Authority) concerning the proposed regulations and the Officer's own suggested revisions. The Board (Authority) may revise the proposed regulations before adoption in response to suggestions made at the hearing without conducting a further hearing on the revisions.

Any person heard or represented at a hearing or requesting notice shall be given written notice of the action of the Board (Authority) with respect to the subject thereof.

No rule or regulation, or amendment or repeal thereof, shall become effective until a certified copy thereof has been filed (in the manner provided by State Law regarding the filing of administrative regulations).

Any person adversely affected or threatened by any rule or regulation of the Board (Authority) may obtain a determination of the validity of the application of such rule or regulation by petition for review (pursuant to appropriate State Law regarding administrative review).

SECTION 5. Local Government.

(a) The Board (Authority) shall exercise all powers and perform all duties as provided for in the Act with regard to any personal information system operated, conducted or maintained by such local government, other political subdivision or combination thereof; or

(b) At the request of any local government, other political subdivision or combination thereof in this State, the Board (Authority) may adopt regulations to: permit the establishment of a local information practices board (authority); govern the operation of such local information practices board (authority); and define the rule-making and review authority of such local information practices board (authority). Such local information practices board (authority) shall be operated by and at the expense of such local government, other political subdivision or combination thereof.

(c) Such local government, other political subdivision or combination thereof may request that the Board (Authority) dissolve a local information practices board (authority).

SECTION 6. Rights of Subjects of Information. The rights of persons on whom the information is stored or to be stored and the responsibilities of the responsible authority shall be as follows:

(a) The purposes for which personal information is collected and used or to be collected and used shall be filed in writing by the responsible authority with the Board (Authority) and shall be a matter of public record pursuant to Section 4.

(b) A person asked to supply personal information shall be informed of all intended uses and of the purpose of all intended uses of the requested information.

(c) A person asked to supply personal information shall be informed whether he may refuse or is legally required to supply the requested information. He shall be informed of any known consequence arising from his supplying or refusing to supply the personal information.

(d) Information shall not be used for any purpose other than as stated in clause (a) of this section unless (1) the responsibile authority first makes an additional filing in accordance with clause (a); (2) the legislature gives its approval by law; or (3) the persons to whom the information pertains give their informed consent.

(e) Upon request to a responsible authority, a person shall be informed whether he is the subject of stored information and if so, and upon his additional request, shall be informed of the content and meaning of the data recorded about him and shown the information without any charge to him. For a six month period after such disclosure, additional disclosures shall be made at the cost of making the disclosure. This clause does not apply to information about persons which is defined by statute as confidential or to records relating to the medical or psychiatric treatment of an individual.

(f) A person shall have the right to contest the accuracy or completeness of information about him. If contested, the person shall notify in writing the responsible authority describing the nature of the disagreement. The responsible authority shall within 30 days correct the information if the data is found to be inaccurate or incomplete and attempt to notify past recipients who have received the inaccurate or incomplete data within the preceding two years (or other desired term) of the inaccurate or incomplete information, or notify the person of disagreement. The determination of the responsible authority is appealable in accordance with (Administrative Procedures Act or procedures in this Act). Information in dispute shall not be disclosed except under conditions of demonstrated need and then only if the person's statement of disagreement is included with the disclosed information.

(g) A person has the right to be free from the storage and continued collection of personal information no longer utilized for any valid purpose.

(h) A person has the right to be free from the collection, storage or dissemination of any personal information collected from anonymous sources except as exempted by the Board (Authority) or statutes.

SECTION 7. Penalties. Civil and criminal remedies should be established consistent with statutes and environment of the State.)

SECTION 8. Common Law. No existing statute or common law shall be limited or reduced by this Act.

SECTION 9. Severability of Unconstitutional Provisions .If any Section, subsection, sentence, or clause of this Act shall be adjudged unconstitutional, such adjudication shall not affect the validity of the Act as a whole or of any Section, subsection, sentence or clause thereof not adjudged unconstitutional.

SECTION 10. Liberal Construction. The provisions of this Act and the regulations promulgated thereunder shall be liberally construed to protect the person's right to privacy and confidentiality.

SECTION 11. Effective Date. This act shall become effective (desired date. This date should allow sufficient time for planning and implementation.).

SESSION SUMMARY

Supporters of some of the sample bills were questioned at great length, and the committee profited from diverse experiences occuring in each of the States. After a detailed examination of the provisions of each bill, the committee attempted to isolate areas of consensus. However, the more specific it became, the more conflict of opinion arose. Nevertheless, the discussions provide helpful insights to would-be sponsors of data banks privacy legislation pertaining to State and local government.

At the outset, Chairman Aronoff outlined structural components needed in most data bank privacy legislation:

1. A statement of purpose.
2. A definition section.
3. A designation of enforcement power.
4. A section establishing the individual's right to see, copy, review and challenge a record about himself.
5. A provision on minimum obligations of record-keeping organizations.
6. Conditions of disclosure and dissemination of information.
7. Exceptions (in some bills), and
8. Civil remedies and general penalties.

Aronoff persistently emphasized the importance of balancing privacy bills with right-to-know statutes. He also consistently pointed to subtleties that are not always immediately apparent—for example, the precise degree of consent needed from the subject of a file before access to or dissemination of information from the file is permitted.

The first witness, Marjorie Eltzroth of Massachusetts, in reading Governor Sargent's prepared statement, pointed out that a wise policy demands that government "put its own house in order" before "pressing the fight for privacy against giant credit bureaus, medical data banks, private educational institutions and the like." The first step in developing the Massachusetts approach to privacy was the creation of an independent citizens' commission, which met for a year and found some basic facts about privacy in State government:

1. There are no minimum standards to insure privacy in existing State laws because of the variance in the statutes.
2. Administrative practices and the regulations interpreting them are more uneven than the chaotic State laws.
3. Agency heads lack knowledge about what information is contained in their computer systems while the systems managers who have that knowledge lack understanding of its value or importance; and
4. Virtually all computerized systems are insecure.

As a result of these findings, some minimum standards were issued and, already, some State agencies are overhauling their information practices.

Nevertheless, Sargent's statement emphasized, State laws will be worthless unless and until the Federal government passes privacy legislation.

In the question-and-answer period that followed, Aronoff noted the general applicability of the Massachusetts model:

First, the State had a commission, a body to investigate what is going on in government and report back to the governor; secondly, an executive order was issued on the part of the governor to speed action forward; and thirdly, comprehensive legislation was drafted along the lines of the HEW guidelines.*

In his testimony, Mike Cullen of California said that two years ago voters in his state

responded to the question of protection of individual privacy by amending our Constitution to include privacy as an inalienable right of all people. By that action, the people of California provided the legislature with a clear message, which reflected a general dissatisfication with the erosion of their personal privacy . . . We'd come to the realization that, like the bald eagle and the blue whale, privacy was becoming an endangered species.

Too easily taken for granted, privacy was being eroded to the degree that it could become a memory rather than a reality. Just as the eagle and the whale are integral parts of our natural ecology, so is privacy an integral part of our social ecology, and the people of California are asking that the assault on it be halted.

With the increasing use of electronic data processing technology in California, Cullen said, "it is apparent that the right of an individual to privacy is contingent upon a modern day factor; that is, computer-related security."

Cullen also noted that the effective universal identifier in California is the driver's license.

* Refers to principles set forth in *Records, Computers, and the Rights of Citizens*, pp xx-xxi. See appendix V.

State Representative William R. Bryant, Jr., reviewed the Michigan bill, which he drafted. He pointed out that privacy legislation was a "kind of a new hot issue, somewhat akin to consumerism, and we are going to have to be careful we don't do things wrong." He said it would affect a lot of people, would have significant cost-related effects, and would change State and local government considerably.

Daniel B. Magraw, the final witness, summarized the key points of the omnibus-type Minnesota bill, which along with the Michigan bill had been included in the pre-Seminar mailing of materials. Three main sections cover:

1. A kind of Bill of Rights giving people access to their records.
2. The promulgation of rules and regulations to apply to State agencies and local governments.
3. The requirement for a report listing personal data banks so public officials know the facts concerning existing systems.

An interesting discovery by Magraw was that virtually every city and county-level file in Minnesota is a "people" file. There seems to be no such thing as a "nonpeople" file. In addition, about 75 percent of these files are classified as public records.

Magraw also spoke of the problem of the use of public records, and the difficulty of telling people in advance how a public record will be used. If records are truly public, anyone can use them for any purpose they wish.

Although it was not a part of the direct charge to the Committee, several members strongly felt that legislatures should examine and re-examine the need of government to collect personal data in the first place. If such need exists, which specific data are relevant and necessary?

This gets to the core of the privacy issue. Assuming that State and local government does have the right to collect some personal information, it was the consensus that comprehensive omnibus legislation covering State and local government record keeping is necessary. The Committee voted issue by issue and reached the following conclusions:

1. A bill should enunciate the five principles of fair information practices recommended by the HEW committee (with one exception), to wit:
   a. There should be no secret record keeping operation.
   b. People must be able to find out what information about them is on record and how it is used.
   c. People must prevent information gathered for one purpose from being used for another purpose without consent. (Several members felt that the term consent must mean "informed" consent. The Committee was unable to resolve whether consent was a mandatory part of the bill, since it raised serious cost questions and questions of practicality. At the very least, the Committee determined that an individual should be made aware that information collected for one purpose has been used or will be used for another purpose.)
   d. People must be permitted to see, amend, and correct their records.
   e. Record-keeping organization must assure the accuracy and reliability of data and prevent misuse.
2. The Committee was evenly split over whether an omnibus bill should apply to the private sector as well as to the governmental sector. For practical and political reasons many people felt that the private sector should be covered in separate legislation.
3. An omnibus bill should cover all information systems, not just automated personal data systems.
4. The bill should cover all "legal persons", not just individuals. (The discussion was too brief to draw a conclusion as to whether there was a real consensus on this question.)
5. An omnibus bill should give special treatment for statistical research records. (There was no attempt to define "special treatment.")
6. An omnibus bill should include criminal offender records. (There were strong dissents on this question.)
7. By a slight majority, the Committee preferred an independent, quasi-judicial board rather than regulation by statute or by an existing State agency or board. (This discussion did not go into depth and the Committee found it difficult to address the issue without specifics.)
8. Conflicts with State freedom of information acts have to be resolved as do possible conflicts with the First Amendment of the Constitution.

The Committee was almost equally divided as to whether the legislature should provide an appropriation to cover the cost to State and local governments of implementing a privacy statute.

The Committee agreed, with some dissent, that the bill should be futuristic rather than retroactive.

CHAPTER 5

LUNCHEON ADDRESSES

Two pertinent addresses supplemented the program of the Privacy Seminar. At lunch on the first day, participants heard an address by Dr. Alan F. Westin, Professor of Public Law and Government at Columbia University. On the second day the Seminar concluded with a luncheon address by State Assemblyman William T. Bagley of California. An abstract of the Westin address is printed below followed by the text of the Bagley address:

LUNCHEON ADDRESSES

Abstract of Luncheon Address by Alan F. Westin

The theme of this presentation is that we have left the decade of early alarms and empirical studies with regard to the "computers-and-privacy" issue and have entered the era of regulation. Moving into the regulatory mode will require a much closer relationship and exchange of views between computer professionals and organizational managers on the one hand, and the public policy makers on the other. Such a new relationship must be built, in considerable part, on close monitoring of the effects of new laws and regulations on the operations, costs, and decision-making processes of organizations so regulated, and on better informed estimates of the likely effects of further proposed regulations.

1. Concerning the emergence of the "databank" issue, general fears about increased capacities for technological surveillance over individuals and groups were voiced in the early 1960's. These increased capacities included physical and psychological surveillance as well as data surveillance. By the late 1960's, this had been thoroughly aired in the mass media as well as in legal, civil liberties, and computer-industry circles.
2. The early alarms developed three basic assumptions as to what were seen as "inevitable" effects of large organizations adopting computers in their keeping of personal records: that it would lead to collecting more extensive and intrusive information about the organization's clients, customers, employees, or subjects; that organizations with computers would exchange personal data more widely with other computerized organizations; and that automation would lead to the creation of more secretive or inaccessible files on persons.
3. The National Academy of Sciences' Project on Computer Databanks (published in *Westin and Baker, Databanks in a Free Society,* 1972) found that the three "inevitable" effects of automation were not yet taking place in the real world of computerizing organizations. Various organizational, financial, legal and technical constraints were keeping the existing patterns of information collection, sharing, and openness-or-secrecy in essentially the same channels—whether those were in harmony or at odds with privacy and due process claims—as had existed in those organizations before automation of files had begun.
4. The NAS study also concluded that a major records-and-privacy debate would be taking place today in American Society even if the computer had not been developed. This is because our society had already become, by the 1950's, such a complex service-oriented, and credential-based social system, and so heavily reliant on formal records, that the *standards* used for judging people and the *procedures* used for making those decisions would have come under fundamental attack in the climate of social upheaval in the 1960's and down to today. It is major challenges to governmental and private-organization use of race, sex, cultural conformity, sexual practices, political activity, and similar exclusionary standards, as well as traditionally secretive and closed decision making practices, that is the real crux of the problem. However, the computer is clearly *accentuating* these issues by increasing the speed, efficiency, and use of automated personal data, and it is increasingly in the setting of large, automated databases that new public policies must be applied.
5. The NAS Report, along with the report of the HEW Advisory Committee on Automated Personal Data Systems (1973), called for regulatory action in the mid-1970's before computer systems became so large and costly, and expanded into more ill-considered uses, that American society might not be able to bring them under effective and cost-bearable controls.
6. The findings of the NAS study and the analysis of the HEW Report are closely paralleled by similar studies and reports in many of the Western parliamentary nations. Conclusions favoring regulatory action have been reached in half a dozen of these countries, ranging from Sweden's National Data Protection Act of 1973 to Britain's policy of relying on codes of principle rather than statute or legal rights. There are substantial reasons why the U. S. should not follow *either* the high-administrative control policy of Sweden or the "no-law" policy of Britain.
7. Our response has been to enact both "rifle-shot" laws such as those dealing with commercial reporting agencies (Fair Credit Reporting Act of 1970) and student records (the Buckley Amendments), and also to pass omnibus statutes based on a blend of the HEW Committee's "fair information practices" approach and the "Bill of Rights" approach championed by Senator Sam Ervin, Jr. and the American Civil Liberties Union. Such pursuit of both single-area detailed laws and jurisdiction-wide fair information acts will be the arena of action among the states during 1975-76.
8. We will need to pay close attention to how the general rules and procedures of any Federal and State privacy statutes work out in practice. This will require technical, legal, and public-policy experts to gather empirical data about money costs, efficiency costs, effectiveness for protecting citizen rights, levels of use, ease of evasion, and other "implementation" matters. Who will do this, how, and through what mechanisms of legislative and public oversight will be critical issues for the next few years.
9. Several pending bills in specific areas—criminal justice information systems, banking privacy and credit reporting, omnibus bills, as well as others—could extend Federal regulation to State and local governments and to the private sector.
10. Finally, computer professionals in particular must be more forthcoming as legislative alternatives and regulatory rules are debated. Many desirable protections of individual rights can be achieved without disruption of socially vital information activities *if* informed concepts are used in the regulatory action. On the other hand, not every demand made in the name of "privacy" or "personal rights" deserves to be written into law as a prohibition of data uses or a limitation on organizational information policies. A society that wishes to pursue the Jeffersonian ideal must recall that he was a champion of knowledge, science, and technological progress as much as he was of personal liberties, and that striking the right balance between these values of a free society should still be our goal.

Luncheon Address of William T. Bagley

THE POLITICS OF PRIVACY

Today's privacy "rage" could very well supplant and certainly has become a sequel to the latter-day demands for "freedom of information." How you can protect both the right of privacy and the public's right to know, and at the same time pass a bill on these subjects at the state level, is the subject to be addressed. We will only allude to the esoterics and then discuss in detail the practical aspect of putting a palatable and thus passable bill together. Thus, the politics of privacy.

Historically, the right of privacy evolved as a "tort"—a civil law where something not in the public domain was brought to the public's attention. Even though true, an invasion of someone's "right of privacy," by making commercial usage of some private event, was held to be a civil wrong and therefore the basis of a civil cause of action.

This tort was late in its arrival into the common law, having something of its genesis in an article by the then Professor Louis Brandeis, 4 Harvard Law Review 193 (1890), who defined privacy as "something all men (and we now would add women) are entitled to keep from public curiosity!"

In those earlier days and until recently the thought of having, or of being the subject of, a dossier was only accorded to the priviledged few. It was even thought of as being desirable. But now the dossier has become democratized, available to about almost anyone, and in computerized profusion. Thus our concern today for the "right of privacy" and necessary protections, but in a vastly different sense.

By now, the participants of this Seminar certainly are aware of the elements of this present day social problem and of the components of the solution. I shall not spend much time relating those elements. Briefly stated, on the problem side of the ledger, we find a proliferation of record-making and record-keeping, the potential and actual linkage of different records, the obvious easy storage and retrieval elements of computerization, the seeming authenticity of "print-outs," and, most important, the depersonalization of the record-keeping process. The answer to the question—where is the record—is of equal importance to what is in it. This illusory aspect, this depersonalization, this inability to "talk to the clerk," all add to and dramatize in the public mind the feeling of fear of potential computer abuses of the right of privacy.

Right or wrong, founded or not, we must recognize that the fear is there in the public mind. It is our job in government not only to prevent the possible abuses, but also, of equal importance, to allay the public fear.

And thus we come up with "solutions" which, when put into law, become substantive rights of citizens in this field. Thus we propose a right of access of individuals to their own records, a right of insertion of corrective materials. We propose a limitation on linkage. We propose "audit-trails" to see who is looking at us. And we propose technological security required to be built into the computer.

I would add that of equal importance or perhaps even of more importance than any of these "rights" is the requirement or the necessity for "identifying" the computer. A large part of the fear would disappear and much of the ominous aura of the computerized age would be dispelled if we could somehow re-personalize record-keeping. That does not mean that we are going back to manual record-keeping. It does mean that we must provide a ready mechanism for finding the computer and, specifically, for finding the named person in charge of computer security and in charge of your record. Then a member of the public can talk to that person and, in the vast majority of instances, gain satisfaction.

And now let us talk about the "politics of privacy," again recognizing some of the problems, some of the pitfalls, and some of the pluses.

NEGATIVE ASPECTS

First of all, in reference to problem areas, let us recog-

nize the basics. In today's society, one new badge of authority is to carry the key to the computer—and we all know how difficult it is to take badges away from people. And, in that context, let us not try to solve all social problems all at once with a single omnibus piece of legislation.

For example, let us assume that one of us, last night, was noted dancing on the stage of the Silver Slipper, and assume that this was made a matter of appropriate record. Regardless of computerization there is not much we can do with that kind of a record, except perhaps to assert our right of insertion and correction by adding to the record: "but she really is a nice lady—she's a friend of my wife and we all play bridge together."

And let us also recognize that for every "computer horror story" that we tell in an effort to propose and propound the protection of the right of privacy, opponents to legislation will counter with their horror stories—most of them couched in terms of cost. But recognize also that you can remove these objections by simply not trying to solve all the problems all at once and by, for example, eliminating expensive audit trail requirements, eliminating the requirement of prior notificaton before records are kept or divulged, and by eliminating any prohibition against linkage of one computerized record with another, without requiring prior consent of the subject. Under a "millennium" piece of legislation, all of these latter components would be important; but one must recognize that by definition the "millennium" cannot be realized in less than one thousand years.

Let me relate some quotes from the opponents of AB 2656 in California. First of all I should state that this was, contrary to my good advice given here, an omnibus bill which covered not only all governmental (state and local) computerized personal data records, but also covered the entirety of the private sector. Parenthetically, I have been asked, in incredulous tones, who in the world could oppose a bill to protect the right of privacy? Who opposes?—just the entire public sector and the entire private sector! That was almost literally true of the bill in its original all-encompassing form. For example:

> The State Department of Finance objected to "excessive costs" in the range of $10 million to $34 million.
>
> The Department of Motor Vehicles told us that they would have to send notices, perhaps annually under the bill, to 14 million licensed drivers in California.
>
> The County of San Bernardino said "your bill would mandate a nightmare of added paperwork to current County procedures."
>
> The Department of Justice states . . . "as a matter of public policy criminal justice agencies should not be subject to its provisions."
>
> Computer Services, Rockwell International . . . "this would be an impossible restriction comparable to crippling the interstate use of telephones, radio transmission and aviation."
>
> Forest Lawn Memorial Parks and Mortuaries . . . "this legislation would interfere with related business activities for which the company-owned computer is being used."
>
> The California State University and College System . . . AB 2656 fails to take into account the unique educational function of our University system."
>
> East Bay Municipal Utility District (EBMUD) . . . "customer billing should be excluded."
>
> Creative Socio-Medics Corp. . . . "medical records, especially mental health records, must be treated as a separate issue from other computerized records."
>
> State Teachers Retirement System . . . "we comply with the spirit and intent of AB 2656, and to impose additional reporting requirements would be unnecessary and result in higher administrative costs."
>
> State Teachers Retirement System . . . "we comply with the spirit and intent of AB 2656, and to impose additional reporting requirements would be unnecessary and result in higher administrative costs."
>
> TRW/Credit Data . . . "the all-encompassing regulations . . . if enacted verbatim would prove detrimental if not destructive to the credit industry without meaningful benefit to individuals in search of credit."
>
> California Highway Patrol . . . "the ability of this Department in providing effective programs in crime prevention will be deterred by passage of this bill."—etc., etc.

I have to say right now that opposition from law enforcement is most formidable. Therefore, the first amendment which I accepted was to exclude law enforcement!

All of the above, in most abbreviated fashion and eliminating a large part of the response from the public and private sector, indicates what you get for trying to bite off more than you can chew. Again, the message is to come up with a simple, palatable and passable piece of legislation—and don't try to solve all of the social ills of the nation in the process.

A caveat, however: please avoid the temptation of one simple solution—that being to close public records. Not only would that solution be counter-productive, but it would also raise the legitimate and understandable wrath of the journalism fraternity.

Let me add a side thought at that point. One of the greatest allies that I had in passage of major freedom of information bills in California was and is the California Newspaper Publishers Association. We must now interest them and their counterparts in the field of protection of privacy. Good social policy and enlightened self-interest would dictate that media representatives join us in our efforts to protect privacy.

The risk, of course, is if they do not join us in a constructive effort, somewhere along the line the forces that impelled the ominous fear referred to earlier may very well cause legislation to pass which will close otherwise opened public governmental records!

Let me emphasize and restate that latter point. Restated, the public's "right to know" and a person's "right of privacy" are not and should not be made to appear to be conflicting rights. They are, instead, and should be made to interact as correlative responsibilities. Our obligation in government, in final analysis, is rather simple, and that is to make the system work. Specifically, our job here is to weave seemingly conflicting rights and responsibilities into a correlative scheme where we preserve both the public's "right to know" and the individual's right of privacy. On first blush that may seem most difficult. But, and again if we choose not to cure all social ills all at once, it is a rather readily attainable goal.

Positive Aspects

On the plus side of the politics of privacy, we should also recognize some basics. This issue, the protection of the right of privacy, is as politically sexy as it is socially necessary. "Everyone is for protecting our right of privacy: the liberals and the conservatives, from the ADA to the YAF, from the Birchers to the Bombers, all are on "our" side. So, first of all, recognize that we have allies—but recognize, also, that we have to organize our allies.

There is another, perhaps subsidiary, public fear. That is the fear of the social security number becoming a universal identifier (UID). In the vernacular, the social security number is becoming more social and less secure. Use, in the nice sense of that word, this public fear to build a constituency. The constituency is there but it is not organized.

Building a Constituency

So let's talk about the mechanics of building a constituency, a basic necessity toward passing a bill. We, of course, want to and should involve the "cause" people, Common or Uncommon. We need and want their support and actually should go out and help organize their support. With a little prodding and prompting, they will realize that this is a cause that also needs their support.

We also need (and they need us) the computer people. Again, a combination of those great forces for good, pro bono publico and constructive self-interest, dictate that the computer industry join forces to pass palatable legislation rather than face the risk of opposing, and ultimately perhaps swallowing, the impalatable.

That latter thought, to bring in and work with the computer people, is not at all impossible—not impalatable. As long as you eschew the impossible, and work with their governmental relations people and their technical people (and also play on their fears a little bit), you will be successful in encouraging their constructive cooperation. All of this, again, is calculated to construct a constituency. Work with the Council of State Governments who can provide both resources and guidelines for your work. Also, do not ignore local government. Some of us at times express our desire for "home rule". Home rule becomes nothing more than a "homey homile" unless we practice the art—bring in, work with, and just plain include local government and local governmental officials in our work. Governmentally, there are many more computerized personnel data banks within the sphere of local government than those operated by the state.

Simplify the Bill

So, after all of that, let's put a pallatible and passable bill together. I recall at least one old saw from law school: Before you think great thoughts, read the statute. Paraphrasing, let me say that after you have thought all of your great thoughts, draft and passable piece of legislation.

Therefore, my rather gratuitous but hopefully not hollow piece of advice, as one who has been through this but did not follow his own advice, is to put together the following simple bill. I would start with a simple privacy "code of ethics" which would provide guidelines and statements of intent but not necessarily the full impact and import of law. That's a good place to start. I would provide a right of access of the subjects of computerized data banks. I would provide the right of insertion (correction) and perhaps some "forum" to determine whether a given item on the record should be deleted. Providing the forum is almost as important (perhaps more so) as providing the actual technical and somewhat ethereal right of deletion.

Start out with just governmental records—do not try to take on the whole world (all of the private sector) all at once. I do not mean to demean the efforts of the social thinkers in this field. These efforts are most important and, in fact, are catalytic to our being here today. However, from the practical standpoint of the politics of privacy and in the vernacular, "you ain't gonna do it all at once."

Avoid the costly items, such as a required audit trail, a required "prior consent" to interconnections, a required prohibition against linkage. These components might very well be initially drafted into an omnibus bill, but be ready to amend them out—quickly.

Eliminate law enforcement—I would eliminate that in my original draft. Recognize that progress in a democratic

society is made very slowly. Recognize also that progress in a democratic society should be made slowly—because, if progress were very rapid the society may not be very democratic.

So the bottom line would seem to be, first in reference to governmental records, to provide the right of access, the right of correction and insertion and some control over interconnection (if only an administrative guideline). There should be some constraints on record keeping itself. There should be some provision for deletion and some provision for shutting down the record-keeping machine. These latter need not be in exact form but could very well be left to administrative action. Remember, another bill can always be passed.

Also recall the absolute necessity for re-personalization of record keeping. My recommendation in this regard is to require both public and private computerized data banks to *register* the fact that they are personalized data banks.

This is not and should not be construed to be a licensing requirement. Remember, we are also interested in protecting First Amendment rights. But the simple fact of registering—with for example the Department of Consumer Affairs or the Secretary of State's office—that you are operating a personal data bank is important in the re-personalization process. A simple and very non-bureaucratic system of registration can be required. All we are interested in is 1) that you operate a computerized personal data bank, 2) what sphere or general area of information is encompassed therein, 3) where is it located (address and telephone number) and 4), most importantly, who—by name—do you call to obtain "relief." The department involved need do no more than keep a record of that information and make sure that an individual citizen can make contact with the computer—and thereby be able to obtain the stated rights of access and correction.

All of this may sound too simple. But the fact is that kind of bill can be passed and the basic rights with which we are concerned can be protected. Having done that—having provided some basic rights of privacy and having established some type of public forum to which a citizen can appeal—we will have done a major part of our job in not only protecting those rights but allaying the public fear which does exist.

All of this can be accomplished long before 1984.

CHAPTER 6

CONSUMER PRIVACY INTERESTS

To address adequately the subject of Consumer Interests in Privacy required a different approach than the mock legislative hearings used as discussion vehicles for other topics during the Seminar. The relaxed and informal approach of a panel discussion seemed to provide the best method for getting at the fundamental questions.

Panel moderater S. John Byington, Deputy Director of the U. S. Office of Consumer Affairs, was joined in the discussion by panelists Joseph L. Gibson, general attorney for MARCOR (parent organization of Montgomery Ward); Theodore Jacobs, Executive Director of the Center for the Study of Responsive Law; John Kehoe, President of Consumer Concerns, Inc., and former Director of the California Department of Consumer Affairs; Kenneth A. McLean, Professional Staff Member of the U. S. Senate Committee on Banking, Housing and Urban Affairs; and Peter Schuck, Director of the Washington Office of Consumers Union.

The pre-seminar materials mailed to participants included the following issue paper, edited for inclusion here:

ISSUE PAPER

CONSUMER INTERESTS IN PRIVACY

Consumer interests in privacy extend to records containing personal information resulting from market place activities such as acquiring property, services, money, insurance, or credit for personal or family uses. The breadth and diversity of consumer transactions and the variety of record-keeping practices associated with them defy easy definition of personal privacy interests, specification of privacy abuses, or prescription of effective remedies against infringements of privacy.

The effective operation of the modern market place requires the collection and appropriate use of consumer-related data. Business decisions affecting consumers based on inaccurate, obsolete, irrelevant and incomplete data can seriously jeopardize the reputation and economic interests of the individual. Misuse of information can similarly produce adverse consequences for the individual. Unrestrained access to and linkages of records on consumers by business have enormous privacy implications.

Recognition that consumers have certain rights of privacy and that businesses should engage in fair information practices prompted Congress to enact the Fair Credit Reporting Act in 1970. This act, however, is limited to credit reporting agencies and thus does not cover the full scope of consumer transactions in the market place. The need for strengthened and broadened protections of consumer privacy interests is receiving increased attention by consumer and business groups and by governments at the federal, state and local levels. Vitally needed is a definition of intergovernmental roles and responsibilities for oversight and regulation of record-keeping practices in the private sector.

Accordingly, the following topics and issues serve as a basis for consideration of this subject.

Privacy Rights in Consumer Transactions

Great quantities of personally identifiable data on consumers are collected, maintained, and distributed in today's market place primarily by companies doing business in more than one state or country. Credit reporting agencies, financial institutions, many retailers, credit card companies, insurers, and other businesses make frequent use of data on individuals which is typically stored in and retrieved from computers. In this area of commerce, individuals are susceptible to—even when they do not actually suffer from—invasions of personal privacy.

What rights should consumers have regarding the collection, maintenance and distribution of information pertaining to themselves?

How should those rights be protected?

How should sensitive data (such as information on sexual habits, abuse of alcohol and drugs, emotional problems) be treated?

Are there special problems with, and consequently the need for special treatment of, certain types of records, including: medical records: telephone records, particularly of long-distance calls; details of travel records; records on individuals' financial transactions maintained by financial institutions?

What is the best role for the states and localities to play in areas where the federal government is already involved, such as the area covered by the Fair Credit Reporting Act (credit, insurance, and employment transactions involving information developed by consumer reporting agencies)?

Cable Television Systems

Certain cable systems have the capacity to survey all residences connected to the system to determine which program is being watched in each home. Individual sets can also be turned on and off from a central source.

Is the most acceptable solution federal legislation prohibiting monitoring of communications entering and leaving a citizen's home via cable television, and forbidding disclosure of identifiable information about the viewing habits of subscribers unless there is a court order?

What role, if any, is desirable and feasible for state and local governments?

Electronic Funds Transfer Systems

Systems are under development allowing immediate at-point-of-sale transfer of payments from consumer to merchant accounts and between financial institutions. The unauthorized disclosure, interception, or use of such data could result in severe invasions of privacy if it revealed a clear picture of a consumer's movements, spending preferences, and personal habits. For such a system, the adequacy of the customary monthly bank statement also needs to be examined, as does the adequacy of present law on bank liability for errors in the recording and use of account information.

A recent federal law establishes a National Commission on Electronic Funds Transfer. What should the Commission do?

What roles are appropriate for state and local governments?

Mail Lists

There is some public concern over both government and private sector production, dissemination, and use of mail lists.

What are the real privacy interests to be protected?

Are there material privacy abuses in the list area?

What about an "opt-out" opportunity for removing one's name from lists?

Should lists developed by government agencies be treated differently from those developed by the private sector?

PANEL SUMMARY

The basic issue raised during the consumer panel discussion was the extent to which consumer interests in privacy *apply* to records containing personal information—records produced by market-place activities such as the acquisition of property, services, money, insurance or credit for personal or family use. The panelists also raised the question of whether or not an omnibus State privacy bill, one designed to affect record keeping and access to such State records, should apply to private sector records, including those maintained by industry, as well as to government records.

One panelist made two distinctions between State and commercial inquiries into private information. The first was that it is economically prohibitive for industry to collect unnecessary personal data. Since government doesn't have this same economic inhibition, there is a greater probability that government will collect more personal data than industry. The second distinction is that anti-trust laws and vigorous competition restrict the interchange of personal information between businesses. Therefore, that panelist believed, personal data obtained by private companies should not be included within the scope of an omnibus State bill.

Another panelist contended that government information gathering involved the application of different principles than commercial information gathering and that they required radically different approaches. For example, State or Federal government records, with certain exceptions, are public, whereas corporate records are generally private.

The core of the issue involves the question of where most of the abuses lie. Some panelists perceived greater abuses in the private sector than in public records keeping. As an example of such abuses, a panelist cited the Federal Trade Commission's (Consumer Credit Division) case against the Retail Credit Company. This case involved the method by which information on individuals is obtained, the frequent inaccuracy of such information, and the unauthorized use of it. Since this seemed to spark the greatest interest, the major portion of the remaining discussion was devoted to credit lending.

The panelists described two types of credit reports. One is a simple report relating to commercial transactions. It involves who you are, where you live, and by whom you are employed. The other type is the investigative report. The greatest number of complaints involve investigative reports such as those requested by life insurance companies trying to find out what kind of person they are about to insure.

The current structure of the credit reporting industry makes it nearly impossible to produce accurate investigative reports. Life insurance companies, for example, not only demand extensive amounts of information about physical characteristics, morals and sex life, but demand such information at the cheapest rate. Compounding the problem, investigators, believing that a percentage of the apples will be bad, work generally under a quota system. That is, they must produce a certain percentage of adverse cases. A credit company may produce a quota of 20 to 25 reports per investigative agent per day, some of which may end up in the "adverse" category whether or not they are adverse in fact. In light of this, many members of the Congress, including the sponsor of the Fair Credit Reporting Act, Senator Proxmire, believe a legislative overhaul of the system is overdue.

A related issue is what role, if any, the States should play. Since different standards are probably needed for the various States, should there be 50 different State credit reporting acts? Senator Proxmire considers Federal legislation as setting minimum standards for the States. An example is the Fair Credit Reporting Act. In that case, experience of the States will be useful at the Federal level in convincing Congress that more protective and innovative measures can be effective and that such measures neither disrupt the flow of credit information for business purposes nor hurt the economy of the States. Experience in California has demonstrated that the Fair Credit Reporting act omits important provisions such as adequate advance notification to the subject of a credit investigation. In addition, some intrastate businesses require protection for the consumer that the Federal bill does not provide.

Therefore, the States may well profit from implementation of State acts like the Federal Fair Credit Reporting Act even engaging in healthy competition with the Federal government. Until the unlikely time that a perfect Federal bill is developed that would solve all the problems at once, the States should not be preempted in this area. Innovative and experimental State fair credit reporting acts, therefore, do not constitute duplicative legislation.

While some panelists saw the profit motive of private industry as a safeguard against abuse in credit reporting, others saw the profit motive as impelling private industry to seek irrelevant information. Even procedural safeguards may not stop abuse. Perhaps some types of highly personal information should be excluded completely by law from the scrutiny of an investigator even though it may bear some indirect relationship to a person's credit-worthiness or insurability.

A recent example is the Federal Home Loan Bank Board's proposed legislation that would prevent institutions under its regulatory control from collecting data concerning the child bearing intentions of families. Such information would simply be precluded from the permissible data that could be used to justify credit decisions.

The current Fair Credit Reporting Act contains no requirements that an individual authorize the investigation in advance. A majority of the panelists agreed that proposed amendments to this act or any proposed State fair credit law should be predicated upon advance disclosure and consensual authorization of the subject. Whether such amendments should proscribe obtaining certain kinds of highly personal information is a separate issue of some difficulty because of the problem of precisely defining such information.

The panelists also discussed the issue of how the caliber of credit investigators could be improved. One panelist contended that professional licensing, whatever the form, is not the answer, because such licensing is often merely a means for a profession to "cartelize" so as to create parties and avoid price competition.

The core of the problem is the structure of the credit reporting industry itself. Pressures are so great to produce large amounts of information of a broad scope at such small cost that many credit investigators will inevitably follow improper practices.

In addition, there are many contributing factors. For example, the profit motive may impel a profit maximizing company to seek a great deal of information, perhaps of marginal value, that may involve invasion of privacy. Another factor is that some investigators are going to exercise a certain amount of natural curiousity. Also, certain undesirable incentives are often built into the investigation process that may have a bearing on an investigator's career advances. This is a basic aspect of the Federal Trade Commission's case against the Retail Credit Company.

Another issue, the relationship between State fair credit laws and the interstate commerce clause, was also raised. Much data gathered by credit reporting firms is of an interstate nature.

A State couldn't completely regulate a credit reporting company doing business in another State. However, a State could effectively regulate the investigatory process. For example, a State could limit the kind of personal information investigators seek for specified purposes.

The subject of mail lists also came up. As defined by the panelists, the basic issue regarding mail lists concerned advance notification as to the purpose and uses for which one's name is on a list. Many persons buy products or provide information without realizing that their names may be sold commercially as a part of a mail list. Solicitations resulting from the use of such mail lists are considered by some to be unwarranted invasions of personal privacy. However, others viewed the receipt of advertisements and solicitations through the mail as constituting an extremely minor form of privacy invasion. Most panelists agreed that the problem, whatever its extent, could largely be cured by providing persons with advance notification as to the potential uses of the list.

CHAPTER 7

SYSTEMS COST AND THE ECONOMIC IMPACT OF IMPLEMENTING PRIVACY LEGISLATION

The Chairman, Dr. Willis H. Ware of the Rand Corporation, Santa Monica, California, introduced the panel of members on systems cost and the economic impact of implementing privacy legislation. The panel members included: Robert Caravella of the Federal Trade Commission and formerly of the Illinois Department of Finance, Jerry Hammett of the Ohio Department of Administrative Services, Peter Herman of the Vermont Department of Budget and Management, and Paul Wormeli of Public Systems, Incorporated, Sunnyvale, California. A sixth panel member, Walter H. Haase, Deputy Associate Director for Information Systems of the U. S. Office of Management and Budget, had been called away to confer on impending Congressional passage of the Privacy Act of 1974. Dr. Ware presented the statement of the panel, which is summarized here.

PANEL SUMMARY

There are no firm data on which to base an estimate of the cost of implementing privacy legislation. The cost will obviously vary significantly with the specific provisions of any proposed measure and with the starting posture of an agency, especially with respect to its position on the safeguarding of information.

The protection of privacy obviously will involve costs, perhaps substantial ones. However, we are not facing a wholly unprecedented situation. There have been other instances where benefits to and protection of our population have required sizable expenditures to cope with the problems generated by our technology, e.g. fire protection and efforts to deal with environmental pollution. Even if the cost is as high as several hundred million dollars per year, the expenditure of one to three dollars per year for each member of our population is neither formidable nor preemptive, especially when compared to the corresponding figure of about ten dollars per person annually for pollution controls. Thus, while we must acknowledge the impact of the cost and strive to minimize it by carefully drafted legislation and by technical innovation, economic considerations, in themselves, should not preclude action on the privacy front.

In considering various components of cost, it is important to distinguish conceptually between the protection of privacy on the one hand and computer security on the other.

Protection of privacy is largely concerned with assuring that accurate, relevant, and timely information about people is used only for stated purposes and in the best interests of each individual. It includes giving the individual both control over how information about him is used and a mechanism for making corrections to the record.

Computer security (or safeguarding of information in a manual system) includes measures that:

Protect the system—including its physical hardware, its personnel, and the data it contains—against either deliberate or accidental damage by a specified threat;

Protect the system against denial of use by its rightful owners; and,

Perhaps most important for privacy considerations, protect information against disclosure to unauthorized users of the system.

While the cost of computer security can, in principle, be ascribed to privacy legislation, such an allocation represents an inappropriate cost accounting approach. Any information system should have safeguards against accidental or malicious damage or misuse of the information it contains, because its very existence indicates that it is relevant and critical to the appropriate functioning of the organization that maintains it. Thus, information system security should be charged to the basic purpose for which the system exists, even though the security measures contribute to protection of privacy. In systems with well-developed security measures, additional requirements for privacy protection are likely to be of modest cost. In systems with lax security, greater levels of expenditure obviously will be necessary.

Organizations faced with implementing privacy policies and procedures are likely to behave in predictable ways: First, they will automatically resist change in long established methods of operating and record-keeping procedures.

Secondly, when changes are required they will utilize the opportunity to effect other modifications and improvements that have been delayed for various reasons and are, of themselves, desirable but have no direct bearing on privacy protection.

As a result of these circumstances, agencies, partly for self-protection, will tend to overestimate costs to include:

Improvements collateral to privacy issues; and

A sizable contingency margin to deal with uncertainties and to allow some bargaining room.

Thus, in trying to work out the particulars of a bill with those who have responsibilities for implementation, legislators should clearly and thoroughly analyze and dissect agency estimates in order to separate cost elements related to privacy, computer security, and/or other types of system modifications. Once this is accomplished, it is important to examine tradeoffs between specific provisions of a proposed bill and the cost associated with them. Small changes in some provisions may have significant economic impact, while costs may be relatively insensitive to others.

In the following examples, cost components associated specifically with computer security measures are excluded:

Cost components that could be relatively insensitive to detailed provisions of a bill exclude those related to:

Requirements for public notice of the existence, content, and use of data systems; and

Personnel training, establishment of methods, administrative arrangements, and disciplinary procedures.

These requirements are fairly fundamental to the establishment of a privacy program, and the expenditure for them will occur largely only once—at the initiation of the program.

Costs that may vary significantly—even dramatically—depending on the detailed language of a legislative proposal, include those related to:

Recording accesses to a record. Do we record all accesses, a statistical sample of them, only those that are exceptions to routine uses of the data, or only those that become of special interest, perhaps because some record suddenly has many accesses to it?

Notice of corrections that an individual makes to his record. Do we send notice of the correction to all past recipients of a record, all recipients within the past two months, one year, five years, or do we only amend the record so that all future recipients will have the corrected data? For some systems, such as those dealing with criminal justice information, should we send notice of corrections to all past recipients with less stringent procedures for handling corrections in other types of systems? Do we send corrections only at the request of the data subject and then only to the past recipients that he specifies?

Requirements for purging records. Does this mean actual destruction of a particular record in a computerized system at a specified time? If so, it is likely to be more expensive than simply blocking all dissemination at a stated time with actual removal of the record later at a more economically-advantageous moment.

Estimating the cost of implementing privacy legislation is obviously intensified by our inability to judge accurately the level of activity to which a record-keeping system will have to respond.

For example, what proportion of the data subjects in a record system will request access to their records? What proportion of those accesses will require amendment to records and notices to prior recipients of information? The experience of one organization in the consumer credit field indicated a substantial initial impact when the passage of the Fair Credit Reporting Act provided expanded opportunities for consumers to challenge their credit files. The comparability of this experience to demands by data subjects for access to state and local government records about themselves is difficult to estimate but it is probably realistic to anticipate at least an initial surge of requests.

The cost of implementing privacy legislation cannot be accurately measured, particularly where there is a lack of dependable information on the number and kinds of record-keeping systems in a particular jurisdiction, and the uses made of them. However, rough estimates based on some data pertaining to the Federal sector indicate that the economic impact, while [illegible] is not unacceptable.

It is possible to identify specific provisions of proposed legislation that could lead to rapid cost escalation and others for which implementation costs could be reasonably determined and controlled.

Legislators, in working with agencies on the formulation of a bill, should insist upon cost breakdowns that relate projected expenditures to specific requirements of the legislation. This approach could reveal proposed system applications that are not directly related to privacy concerns. Existing capabilities in information technology are adequate to develop cost breakdowns that are accurate enough, according to specific features of a bill.

The absence of privacy legislation can entail actual monetary as well as social costs. With adequate privacy safeguards, some consolidation of record systems with attendant economies of scale would be palatable.

Some activities associated with implementing privacy legislation may be more difficult to accomplish with a manual record-keeping system than with a computerized one, and vice versa. Proposed legislation may have to distinguish between treatment of records in these two types of systems, raising additional cost considerations.

Data that have not been collected cannot be abused. Consideration of privacy legislation provides an opportunity to review a state or local government's authority for collecting personal data and to weigh the social value of maintaining certain types of information against the feasibility and cost of instituting appropriate privacy safeguards.

Similarly, the cost to safeguard record-keeping systems will depend upon resolution of questions of social policy, e.g. decisions to establish socially acceptable ways of using existing data. For example, if it is appropriate from the standpoint of social policy to combine data about welfare recipients with tax records to monitor abuse, then cost savings might be realized through applying safeguards to a single system of records rather than to two separate ones.

In view of the many uncertainties surrounding economic aspects, it may be cost-advantageous to have privacy legislation that authorizes substantial use of administrative rulemaking for establishing specific implementation procedures. The regulatory approach certainly should provide greater flexibility for effecting improvements identified by experience than the legislative or judicial routes.

Similarly, it might be wise to begin with a legislative proposal that specifically does not attempt to solve all problems involved in the protection of personal privacy at once. Initial legislation might be regarded as a basis for learning, with a stipulated agreement that it will be amended in relevant ways, as experience dictates. Thus, a privacy bill should include provisions for feedback of operating information and periodic assessment of the program's cost and effectiveness as it progresses.

PANEL SUMMARY

During the brief period for questions and comments, the following points were made:

A question from the floor inquired about the availability of data associated with implementing the Fair Credit Reporting Act provision that permits a consumer to challenge information in his credit file. Replies from the panel indicated that dependable data of this kind are difficult to obtain, probably because of the credit industry's sensitivity to questions about the accuracy of their records and also because of the proprietary nature of the information. It was suggested that the Federal Trade Commission may have materials on the cost of administering the Act.

In response to a request for reference materials that would assist record-keeping organizations in estimating costs related to privacy and security measures, a document prepared as part of the IBM/State of Illinois Project SAFE effort was mentioned. The publication, entitled *The Elements and Economics of Information Privacy and Security*, contains a checklist of cost considerations. Possibly an interested organization, such as the National Association for State Information Systems, would be willing to prepare a bibliography that pulls together documentation on cost issues from various sources. Also, there is a need for a similar effort to develop a set of uniform definitions of terms related to privacy and security matters. Such a compilation would enhance communication among all those involved in or affected by privacy legislation and programs.

Another cost consideration relates to problems that could result from different or conflicting provisions of privacy statutes in various jurisdictions, e.g. in instances where personal data may be appropriately transferred across state lines.

Concerns were expressed that both public and private sector organizations would withhold or delay new or improved services to consumers because of the costs of safeguarding personal data systems. Panel members felt that it was more likely that the costs would be passed on to the public/consumers in the form of increased taxes or, in the private sector, higher prices.

CHAPTER 8

A STRATEGY FOR COOPERATIVE FEDERAL-STATE-LOCAL PRIVACY PROGRAMS

A panel organized from among the participants made recommendations, which resulted from the discussions and proceedings of the Privacy Seminar, for a strategy pointing toward cooperative Federal-State-local privacy programs. Serving with Panel Chairman Lee M. Thomas, Executive Director of the South Carolina Office of Criminal Justice, were Indiana Representative Kermit Burrous; Assistant Attorney General Alan MacDonald of Massachusetts; Michigan Senator Robert Vander Laan; Howard Kaiser, Director of Data Processing for the State of New York; Mayor Tom Moddy of Columbus, Ohio; Freddye Petett, Administrative Assistant to the Mayor of Portland, Oregon; Justice Robert Utter of the State of Washington; and California Assemblyman William Bagley.

Meeting in plenary session, the Seminar participants considered and adopted several of the panel recommendations. The panel suggested that these be given wide dissemination along with the working papers and summary record of the proceedings. The following recommendations were adopted:

RECOMMENDATION

1. Lest State and local interests be forgotten or reduced to after-the-fact expression, there is an overwhelming necessity for a joint and cooperative implementation strategy for privacy programming among Federal, State, and local governments.

2. A single, coordinating entity should be established for Federal privacy programs.

3. Within one year, each State Governor should call for a conference on privacy and confidentiality to provide a full discussion of the issues by executive, legislative, judicial, and private sector leaders. From such a conference, each State should develop its own unique strategy for the development of privacy programs.

4. Private business interests must be recognized and dealt with in the development of State legislative programs. Such interests should be present at any Governor's conference on privacy and confidentiality.

5. There should be a coordinated effort by State and local, public and private interest groups to develop a mechanism to assure that privacy issues are addressed in a comprehensive fashion. This effort should include broad legislation to enable local governments to develop their own approaches to privacy in concert with State-wide principles.

6. The dissemination of information and the provision of technical assistance for privacy programming should be actively pursued through the Domestic Council Committee on the Right of Privacy and appropriate public interest group coordinating bodies.

Appendix I

PRIVACY—A PERSPECTIVE

by Alice McCarty *

The protection of personal privacy has emerged as a major public policy issue largely within the past decade. A brief look backward, nevertheless, reveals numerous instances of earlier expressions of concern by legal authorities and articulate spokesmen of both the public and private sectors of our society about the invasion of individual privacy.

As far back as 1879, Judge Thomas M. Cooley in his *Treatise on the law of Torts* wrote of a person's "right to complete immunity: to be let alone." An article published in the *Harvard Law Review* in 1890 by Samuel D. Warren and Louis D. Brandeis, entitled "The Right to Privacy," has become a classic and perhaps is the most often quoted as an example of early interest in this subject. The authors were concerned about non-governmental threats to privacy exemplified by a new form of "record-keeping" in their day — photography — and the rights of individuals to sue if they felt their privacy had been invaded. In 1927 Brandeis, then a Justice of the Supreme Court, in a dissenting opinion in Olmstead v. United States wrote that "every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."

In the first half of the 20th century, the rapid development and use of information-gathering and surveillance devices and of such tools for personal assessment and analysis as personality tests and polygraphs prompted occasional protest from public officials, aggrieved individuals, and the press. However, it was not until the mid-1960s that the loss of personal privacy became a matter of widespread concern. This fear resulted from such factors as:

Government demands — appropriate or not — for more information about individuals to carry out its planning, programming, budgeting, statistical, research and analytical responsibilities;

Burgeoning private sector activities in research, market analysis and procedures for handling economic transactions—involving financial institutions, consumer-reporting agencies, the credit card industry, and insurance organizations;

Evidence that the social security number and other types of personal identifiers could be or were used to compile, check, and cross-reference personal data in ways unexpected by and often unknown to the individuals involved;

The inability of individuals to determine readily what records were kept about them, who had access to the records and for what purposes, and whether the records were accurate;

The impact of modern information processing technology with its capabilities to handle, process, store, manipulate and combine data in countless ways, and at almost incomprehensible speed.

About the same time — the mid-1960s — a Federal proposal for a National Data Center was abandoned after press and public outcries about its potential as a first step toward George Orwell's 1984 — and numerous law review, journal and newspaper articles, as well as popular books like *The Naked Society* and *The Privacy Invaders* — began to appear. In 1967 Alan F. Westin, Professor of Public Law and Government at Columbia University, published *Privacy and Freedom,* a detailed treatment of the historical, legal, political, and sociological aspects of privacy. This was followed over the next few years by a number of other studies and publications which have helped to focus public attention on personal privacy issues, including *On Record: Files and Dossiers in American Life,* 1969, edited by Stanton Wheeler; Arthur Miller's *Assault on Privacy,* 1971, and James B. Rule's *Private Lives and Public Surveillance: Social Control in the Computer Age,* 1974.*

Particularly deserving of mention are two landmark studies completed in the early 1970s. *Databanks in a Free Society,* the report of the National Academy of Sciences' Project on Computer Databanks, 1972, by Alan Westin and Michael Baker,

* Alice McCarty is Director of Research for the Domestic Council Committee on the Right of Privacy.

* These and other important reference documents are included on the Reading List (Appendix V).

pointed out that the computer's new capabilities had not yet led inevitably to major changes in organizational patterns of information gathering, manipulation or dissemination; in computerizing their files, organizations — public and private — had generally adhered to their traditional administrative policies on the handling of data. However, computers had brought about a dramatic expansion of information networks with attendant implications for the invasion of privacy; thus, the time had come to consider new legislative, administrative and judicial measures to define and assure rights of privacy and due process.

The second study was sponsored by the U. S. Department of Health, Education and Welfare and conducted by the Secretary's Advisory Committee on Automated Personal Data Systems. In its report, *Records, Computers, and the Rights of Citizens,* 1973, the Committee concluded that it was important to implement a concept of mutuality between record-keeping entities and data subjects. It recommended that record-keeping organzations adhere to five fundamental principles of fair information practice — concepts that have had a major impact on many privacy efforts since undertaken.

During the 1965-72 period, privacy concerns gained considerable visibility in Congress with consideration given to proposals dealing with such subjects as the regulation of Federal data banks, surveillance methods of the military and Federal law enforcement agencies, commercial credit bureaus, census questions, unsolicited mail, and the privacy of Federal employees. During this period Congress enacted two major laws that addressed directly the question of personal privacy — the Omnibus Crime Control and Safe Streets Act of 1968, which contained provisions to limit the legal use of wiretaps, and the Fair Credit Reporting Act of 1971. The latter established procedures whereby an individual can be informed of the nature and substance of information maintained about him by a consumer-reporting agency and can take action to amend his record. (Amendments to strengthen the presently limited safeguards in the Act have been introduced in the 94th Congress.)

The 93rd Congress has been called the "Privacy Congress," principally because approximately 250 bills were introduced between 1973-74, relating both to the issues mentioned above and to others such as criminal justice information, bank records, social security numbers, health records, income tax returns, and telephone communications. That Congress enacted two major privacy measures — the Family Educational Rights and Privacy Act of 1974 (P.L. 93-380) and the Privacy Act of 1974 (P.L. 93-579).

The former, often referred to as the Buckley Amendments, permits parents to have access to school records about their children (and students over 18 have access to such records about themselves), and sharply limits the disclosure of school record information to outside parties.

The Privacy Act of 1974, effective September 27, 1975, establishes individual rights and agency obligations with respect to personal data in systems of records maintained by Federal agencies. It requires each agency to publish an annual notice describing each system under its control from which information about individuals is retrieved in identifiable form; to meet certain conditions for disclosing personal information without the data subject's consent; to establish procedures whereby an individual may review and challenge information in a record about himself; and to limit its record-keeping to information necessary to accomplish an agency function required by law or Presidential order.

Further, the Act places a moratorium on the authority of Federal, State, and local government agencies to compel an individual to disclose his social security number unless required by Federal or State statutes, or by Federal or State regulation adopted prior to January 1, 1975, in connection with the operation of an existing record-keeping system. The Act also establishes a Privacy Protection Study Commission to review and analyze a wide range of issues related to personal privacy, including the need for Federal legislation applicable to State and local government records and records maintained by private organizations. (See Appendix XVII for further discussion of the Privacy Act.)

During the last Session of that "Privacy Congress," in early 1974, the President established the Domestic Council Committee on the Right of Privacy under the chairmanship of the Vice President. Its members are the Secretaries of the Departments of the Treasury; Defense; Commerce; Labor; Health, Education and Welfare; the Attorney General; and the heads of 5 additional agencies — the Office of Management and Budget, the Civil Service Commission, the Office of Consumer Affairs, the Office of Telecommunications Policy, and the General Services Administration. The Committee's charge is to consider and recommend prompt action to assure a proper balance between the record-keeping capacity of public and private organizations and the individual right to privacy. Wiretapping and electronic surveillance is excluded from the Committee's broad mandate since those subjects are currently under study by the National Commission for the Review of Federal and State Wiretapping Laws.

To achieve its objectives the Committee was made responsible within the Administration for developing and coordinating agency views, policy recommendations, and specific legislative and administrative initiatives that affect the way information about individual Americans is collected, recorded, used, and disseminated.

The Committee has endorsed initiatives in such areas as military surveillance of civilian political activities, criminal justice information, electronic funds transfer systems, the confidentiality of taxpayer records, Federal mail lists, customer records in financial institutions, Federal employee rights, and security guidelines for Federal computers and communications systems. Its staff has worked with interagency task forces, individuals and groups outside the Federal Government, members of Congress, and Congressional Committee staffs toward the implementation of these initiatives and others reflected in provisions of the Privacy Act and the Buckley Amendments. Current projects are concerned with the need for a Federal policy on the use of the Social Security number as a personal identifier and the need for strengthened privacy safeguards for employee records, health records, welfare records, and statistical and research data.

Other recent activities at the Federal level with implications for personal privacy include two Executive orders to limit Agriculture Department and White House access to Federal tax return information and the establishment of national study commissions on electronic fund transfers, Federal paperwork, and the publication of human research subjects.

Much of the concern about and action on privacy issues has been at State and local government levels and in the private sector. Many State statutes and regulations as well as local ordinances, some of which have been on the books for many decades, pertain to the collection, dissemination and use of personal data. Laws concerning medical and school records are the most common, while others deal with criminal justice information, the use of wiretaps and polygraph tests, bank records, credit transactions, and public assistance records. Minnesota, Utah, and Arkansas have fair information practice laws that limit the collection and use of personal data maintained by state agencies, require notice of the kinds of personal data maintained by the State, and provide individuals an opportunity to review and, where necessary, correct records about themselves. Minnesota has recently amended its initial statute after almost a year of operating experience. In May 1974, Oklahoma enacted a statute to prohibit new uses of the Social Security number by State agencies. More than 100 privacy-related bills were introduced in State legislatures during 1974, with about 85 measures proposed at this writing in 1975.

In addition, at least seven States have established special commissions or boards to study privacy concerns within their jurisdiction and to examine the need for new State laws or other actions to protect personal privacy.

In the private sector, many business and social science organizations and professional/technical groups have demonstrated leadership in efforts to safeguard personal privacy. They have implemented policies on record-keeping that protect their em-

APPENDIX I

ployees, customers, or members and have sponsored studies, conferences, and publications on various aspects of the privacy issue. Examples include a six-volume study on data security carried out at four study sites with the support of the IBM Corporation; a national conference on the confidentiality of medical records sponsored by the American Psychiatric Association and other health organizations; and the voluntary adoption of codes of conduct by some associations representing the information processing disciplines.

Private organizations as well as public agencies necessarily are devoting increasing attention to the economic impact of modifying record-keeping practices and applying the privacy safeguards and security measures that are being mandated or recommended through legislation and administrative or voluntary action. A few studies and analyses of cost issues are becoming available, including Robert C. Goldstein's *The Cost of Privacy: Operational and Financial Implications of Databank-Privacy Regulation* (Boston, Mass., Honeywell Information Systems), 1975, and a publication of the State of Illinois-IBM Corporation's Project SAFE, entitled, *The Elements and Economics of Information Privacy and Security* (Springfield, Illinois: State of Illinois, Project SAFE), 1974.

Every indication is that privacy issues will continue to occupy a place of prominence with the American people and that efforts to regulate the collection, maintenance and use of personal data will accelerate. At this writing, pending in the Congress are nearly 100 bills concerning such issues as criminal justice information systems, the disclosure of data on taxpayers to third parties (including other government agencies), investigatory access to bank records, and the surveillance of citizens by military and civilian agencies. As mentioned above, nearly as many have been introduced in the 1975 sessions of State legislatures. Privacy-related activities of private organizations continue to expand in anticipation of governmental action to control record-keeping practices in that sector. Experience gained under the Privacy Act of 1974 and similar State fair information practice laws and the findings of the Privacy Protection Study Commission undoubtedly will have a major impact on future legislation, administration, and voluntary initiatives.

Appendix II

GLOSSARY OF FREQUENTLY ENCOUNTERED TERMS

Personal privacy and related concepts, such as confidentiality and data security, lack stable definitions, particularly as they relate to the handling of recorded information. Progress in defining the legal, technical and administrative implications of privacy safeguards policy has been surpassed by computer and communciations technology advances that eradicate barriers of time and distance in information processing. Therefore, without claiming finality and conclusiveness of definition, this glossary attempts to describe various current meanings assigned to terms frequently encounterd in discussions of personal privacy issues.

Personal Privacy: This is a concept having constitutional, common law, and social-psychological roots. As commonly used, it may connote: (1) *substantive* rights, stemming from specific legislative enactment and court rulings, e.g., the physician-patient privilege, the Supreme Court rulings on abortion and contraception, the common law remedies against malicious libel and slander, and the misuse of an individual's name or likeness; (2) a *value judgment,* e. g., a conviction about the extent to which government should regulate or inquire into private conduct; or (3) *due process guarantees,* e. g., the 4th Amendment requirement of warrants prior to seizure of personal property.

Fair Information Practice Principles: These are basic premises that seek to assure that individuals, solely or collectively, are able to influence when, how, and to what extent information about them will be collected, maintained, used, and disseminated by record-keeping organizations. Basic premises with respect to government record-keeping operations include the following:

An agency should collect only personal information that is necessary for the performance of functions authorized by law.

An agency should advise the individual of the purpose for which personal information about him is collected and of any consequences of providing or not providing the information.

An agency should periodically give public notice of the existence and character of systems of records containing personal information.

Unless authorized to the contrary for sound public policy reasons, an agency should permit an individual to have access to his record and to challenge its accuracy, relevance, timeliness and completeness.

An agency should adopt restraints on the disclosure of personal information that are conditioned by considerations of the purpose for which the information was collected.

An agency should maintain personal information with such accuracy, relevance, timeliness and completeness as is necessary to assure fairness in any determination affecting an individual's rights and benefits.

An agency should take reasonable precautions to assure the security and integrity of personal information against damage, misuse, theft and loss.

Personal Information (or Personal Data): This term often encompasses all information that describes anything about an individual, such as identifying characteristics, measurements, or test scores; evidences things done by or to an individual, such as records of financial transactions, medical treatment, or other services; or affords a clear basis for inferring personal characteristics of things done by or to an individual, such as the mere record of his or her presence in a place, attendance at a meeting, or contact with some type of service institution. Another and somewhat more restrictive definition would be any information that is or can be retrieved from a record or record-keeping system by reference to the name, number or some other identifying feature (e.g., fingerprints) associated with the individual to whom the information pertains.

Confidentiality: This is a loose concept that minimally connotes some commitment to withhold from unauthorized users information obtained from or about an individual or institution. In some cases, the subject of the information may be considered an unauthorized user; in others, the universe of authorized users may be broadly described ("any State agency") or redefineable at the discretion of the holder of the information ("whomsoever the Secretary shall designate"). A principal objective of recent privacy legislation has been to give the concept of confidentiality an operational meaning, e.g., by requiring that the authorized users of information be identified in a public notice or in a statement to data subjects at the time of data collection.

Data Security: This is a descriptive term that connotes the degree and means by which information and the machines and facilities for processing, storing and transmitting it are protected from loss and unauthorized access or modification.

Data Linkage: This refers to the combining, cross referencing, or comparison of information in two or more records.

Administrative Record: This is any personal information preserved by an organization for future use or reference

APPENDIX II

that is or may be used to make a decision about the rights, character, opportunities, benefits, or liabilities of the individual to whom it pertains.

Statistical Reporting or Research Record: This refers to personal information maintained by an organization solely for analytic purposes and which, therefore, is *not* used and may not be used to make a decision about the rights, opportunities, benefits, or liabilities of the individual to whom it pertains.

Appendix III

AGENDA

Seminar on Privacy Cosponsored by the Domestic Council Committee on the Right of Privacy and the Council of State Governments

December 16-17, 1974

Monday, December 16

9:00 - 9:45 a.m.	Plenary Sessions— Welcome, Discussion of Seminar Objectives, Orientation to Seminar Format
10:00 - 12 Noon	Mock Legislative Committee Sessions to Consider Draft Privacy Legislation Pertaining to: 1. State and Local Government Data Banks 2. Public Employee Records 3. Criminal Justice Information Systems
12:15 - 1:30 p.m.	Luncheon— Speaker: Dr. Alan F. Westin, Professor of Public Law and Government, Columbia University
1:30 - 3:45 p.m.	Mock Legislative Sessions Resume, Concluding with Summary of Views Expressed and Recommendations Developed
4:00 - 5:30 p.m.	Plenary Session— Panel Discussion on Consumer Privacy Interests

Tuesday, December 17

9:00 - 12:00 p.m.	Plenary Session
9:00 - 10:00	Reports from Legislative Sessions— Discussions
10:15 - 11:00	Panel on Systems Cost and Economic Impact of Implementing Privacy Legislation
11:00 - 12 Noon	Presentation of an Implementation Strategy for Cooperative Federal-State-Local Privacy Programs
12:15 p.m.	Luncheon— Speaker: Assemblyman William Bagley, California
2:00 p.m.	Adjournment

CONTINUED

1 OF 2

Appendix IV

ATTENDANCE LIST

Seminar on Privacy
December 16–17, 1974
Mayflower Hotel

Alaska

Reprensetative William Parker

Senator Bill Ray

Arizona

Major Frank Kessler
Tucson Police Department

Senator John Roeder

California

Chief Deputy Attorney General
Charles A. Barrett

Larry Bolton
Legal Counsel
Office of Criminal Justice Planning

Deputy Attorney General
Michael Franchetti

Terry Hatter
Executive Assistant to the Mayor

O. J. Hawkins
Executive Director
Search Group, Incorporated

Ben Lew

Seth Thomas
Assistant Director
Department of Justice

Jack Walsh
Supervisor
San Diego County

Delaware

Norma Handloff
Executive Director
Delaware Agency to Reduce Crime

Florida

James B. Ueberhorst
State Court Administrator

Georgia

Walter Boles
Director
Georgia Crime Information Center

Amos Southerland, Director
Information Computer Services Division
Department of Administrative Services

Idaho

Fred K. Grant
Court Specialist
Law Enforcement Planning Commission

Illinois

Allen Flaum
Executive Director
Governor's Commission on Personal Privacy

Jeff Goldsmith
Special Assistant to the Director
Bureau of the Budget

Gary McAlvey
Chairman
Search Group, Incorporated

Indiana

Reperesentative Kermit Burrous

Michael Carroll
Deputy Mayor
Indianapolis

Chief Judge James Richards

Raymond W. Rizzo
Executive Assistant
Office of the Governor

Iowa

Representative Philip Hill

Kansas

Representative Don Everett

Representative Richard Loux

Kentucky

George A. Bell
Staff Assistant
National Association of State Budget Officers
Council of State Governments

Dr. Jack D. Foster
Project Director
State's Criminal Justice Information and Assistance Project

Richard E. Jaggers, Jr.
Director
Division for Management Systems

Charles Trigg
Assistant Director
National Association of State Information Systems

Carl Vorlander
Executive Director
National Association of State Information Systems

Louisiana

Speaker E. L. Henry

Maine

Charles Acker
Director
Mental Health Information Project

Maryland

Larry N. Blick
City Manager

Jane Cerza
Special Assistant
Office of the Governor

Carl Everstine
Director
Department of Legislative Reference

Delegate J. Hugh Nichols

Richard Wertz
Executive Director
Governor's Commission on Law Enforcement

Chad Young
Special Assistant
Office of the Governor

Massachusetts

Nancy French
Computerworld

Robert R. J. Gallati
Professor
Northeastern University

Alan MacDonald
Assistant Attorney General

Michigan

Einar Bohlin
Supreme Court Administrator
Representative Perry Bullard

Glenn Goodman
Director
Bureau of Management Sciences

Thomas F. Taylor
County Commissioner
Wayne County

Senator Robert VanderLaan

Minnesota

Richard L. Brubacher
Commissioner of Administration

Representative John Lindstrom

Richard F. Scherman
Director
Pretrial Services

Senator Robert Tennessen

Missouri

Robert Gruensfelder
Executive Director
MLEAC

Gary Rath
Consultant
EDP Coordination Division
Office of Administration

Charles Schaffer
State Information Systems

Nebraska

Senator John Cavanaugh

Senator Roland Luedtke

New Jersey

Hubert Williams
Police Director

New York

Judge Benjamin Altman
Executive Director
Mayor's Criminal Justice Coordinating Council

Rheta Bank
Director
Educational Services
Rockland Research Center

Commissioner Donald Bardell
Department of Motor Vehicles

Jack David, Esquire

H. Howard Kaiser
Director
Data Processing

Kenneth D. Molloy
Coordinator
Office of Federal and State Aid

Martin F. Richman
Chairman
Committee on Federal Legislation

North Carolina

Bill Biggers
Administrative Assistant to the Secretary
Department of Administration

Bruce Lentz
Secretary
Department of Administration

Bruce Merrett
Manager of the ADP Planning Section
Department of Administration

Donald R. Nichols
Administrator of Law and Order Division
Department of Natural and Economic Resources

Ohio

James B. Mcmanama
Manager
Data Processing Center

Tom Moody
Mayor of Columbus

Oklahoma

Senator Jerry Pierce

Oregon

Senator Elizabeth Browne

Duke Morton
Manager of Program Evaluation
Department of Human Resources

Freddye Petett
Administrative Assistant
Office of the Mayor

Pennsylvania

Deputy Attorney General Morris Solomon

Rhode Island

Steve Cohen
Intern
Policy and Program Review

Oliver L. Thomson, Jr.
Administrative Assistant
Legislative Affairs Council

South Carolina

Lee M. Thomas
Executive Director
Office of Criminal Justice

South Dakota

Representative Dennis MacFarland

Tennessee

Robert W. Chaffin
Director
Division of Intergovernmental and Employee Relations

Joan Vollmer
Deputy Commissioner of Personnel

Texas

William E. Roberts
Director
Information Systems Department

Dick Strader
Senate Research Staff

Virginia

Roberta Colbertson
Special Assistant
Cabinet of the State of Virginia

Samuel A. Finz
Director
Office of Research

Senator Joseph V. Gartlan, Jr.

Douglas Harman
Deputy County Executive

Bert Johnson
County Manager

Howard Middleton
Assistant City Attorney

Ben Ware
Computer System Development
Office of Research

Washington

Saul Arrington
Administrator
Law and Justice Planning Office

Justice Robert Utter

West Virginia

Delegate Phyllis Given

Wisconsin

Representative Lloyd A. Barbee

Lawrence Barish
Research Analyst
Legislative Reference Bureau

Washington, D.C.

Joseph Alviani
General Counsel
National Conference of State Criminal Justice Planning Administrators

Larry Bailey
Assistant Executive Director
U. S. Conference of Mayors

Barbara Bayly
Executive Assistant to Congressman Koch

Louise G. Becker
Analyst in Information Science
Congressional Research Service
Library of Congress

Robert L. Chartrand
Specialist in Information Service
Congressional Research Service
Library of Congress

Stephen M. Daniels, Minority Counsel
Government Operations Committee
U. S. House of Representatives

James H. Davidson
Counsel
Government Operations Committee
U. S. Senate

William R. Drake
Program Administrator
Criminal Justice
U. S. Conference of Mayors

Margery Elfin
National Wiretap Commission

Jeffrey L. Esser
Administrative Assistant
National Conference of State Criminal Justice Planning Administrators

Ed Gallagher
National Wiretap Commission

Thomas Graves
Special Assistant for Intergovernmental Relations
Office of Management and Budget

Chief Judge Harold Greene
Superior Court

Alice Grisham
Information Coordinator

David Guarino
Governor's Intern - Texas

Marilyn Harris
Professional Staff Member
Government Operations Committee
U. S. Senate

Tim Honey
Legislative Counsel
National Association of Counties

Jerry Hutton
Congressional Research Service
Library of Congress

Samuel Laudenslager
Assistant Deputy Project Director
Criminal Justice Section
American Bar Association

William Lytton
Counsel to Senator Percy

Anthony McCann
Criminal Justice Specialist
National Association of Counties

Earl S. Mackey
Executive Director
National Conference of State Legislatures

Arnold Malech
Executive Officer
District of Columbia Courts

Ronald J. Nolfi
Director
Statistical Analysis Center

Vincent Puritano
Intergovernmental Relations and
Regional Operations
U. S. Office of Management and Budget

Clark Renninger
Staff Assistant
Institute for Computer S/T
National Bureau of Standards

Erwin S. Rhodes
American Bar Association

Ronald Tucker
Counsel to the Criminal Justice Project
U. S. Conference of Mayors

Donald Newman
Director
Indiana Washington Office

RESOURCE PERSONS

Criminal Justice Information Systems Session

Chairman
Attorney General Robert H. Quinn
Commonwealth of Massachusetts

Witnesses
Mr. Richard N. Harris
Director
Division of Justice and Crime Prevention
Commonwealth of Virginia

Mr. Edward J. Kelly, Attorney
Whitfield, Musgrave, Selvy, Kelly & Eddy
Des Moines, Iowa
Chairman of the Iowa State Bar Association
Special Committee on Traffic Records and
Criminal Information Systems (TRACIS)

Mr. Thomas Madden
General Counsel
Law Enforcement Assistance Administration
U. S. Department of Justice

Mr. Archibald R. Murray
Commissioner
Division of Criminal Justice Services
State of New York

General State And Local Government Data Banks Session

Chairman
Senator Stanley J. Aronoff
State Senator
State of Ohio

Witnesses
Representative William R. Bryant, Jr.
House of Representatives
State of Michigan

Assemblyman Mike Cullen, Chairman
Assembly Committee on Efficiency and Cost
Control
State of California

Mr. Daniel B. Magraw
Assistant Commissioner
Department of Administration
State of Minnesota

Marjorie Eltzroth
Executive Director
Governor's Commission on Privacy and
Personal Data
Commonwealth of Massachusetts Representing
Governor Francis W. Sargent

Public Employees Records Session

Chairman
Eric Plaut, M. D.
Deputy Commissioner
Department of Mental Health
State of Indiana

Witnesses
Mr. Gary D. Bearden, Director
Bureau of Manpower Information Systems
U. S. Civil Service Commission

Mr. Harry B. Douglas, Jr.
Equal Employment Opportunity Coordinator
State of Florida

Mr. Sheldon Mann, Economist
Research Department
American Federation of State, County,
and Municipal Employees

Consumer Interest Panel

Chairman
Mr. S. John Byington
Deputy Director
U. S. Office of Consumer Affairs

Panelists
Mr. Joseph L. Gibson, General Attorney
MARCOR (parent organization for Montgomery
Ward & Co.)

Mr. Theodore Jacobs, Executive Director
Center for the Study of Responsive Law

Mr. John Kehoe, President
Consumer Concerns, Inc.
Sacramento, California
(formerly Director of the Department of Consumer
Affairs, State of California)

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

Mr. Peter Pryor, Chairman
New York State Consumer
Protection Board

Mr. Peter Schuck
Director, Washington Office
Consumers Union

Panel On Systems Cost And Economic Impact Of Implementing Privacy Legislation

Chairman
Dr. Willis H. Ware
Corporate Research Staff
The Rand Corporation
Santa Monica, California

Panelists
Mr. Robert Caravella
Information Systems Center
U. S. Federal Trade Commission

APPENDIX IV

Mr. Walter Haase
Deputy Associate Director
for Information Systems
U. S. Office of Management and Budget

Mr. Jerry Hammett
Deputy Director
Department of Finance
State of Ohio

Mr. Peter Herman
Principal Analyst
Department of Budget and Management
State of Vermont

Mr. Paul Wormeli
Vice President
Public Systems, Inc.
Sunnyvale, California

STAFF

Domestic Council Committee on the Right of Privacy

Eileen M. Bartscher
Research Assistant

Kent S. Larsen
Director of Public Information

Douglas Lea
Consultant

Norman A. MacNeill
Legal Assistant

Dawn M. MacPhee
Legal Assistant

Alice H. McCarty
Director of Research

Douglas W. Metz
Acting Executive Director

David P. Milanowski
Research Assistant

Janet K. Miller
Research Assistant

Carole W. Parsons
Associate Executive Director

George B. Trubow
General Counsel

Council of State Governments

Brevard Crihfield
Executive Director

J. Keith Dysart
General Counsel

Kathleen B. Johnson
Office Manager

Mollie O. Zahn
Staff Assistant

National Conference of State Legislatures

Paul E. Sweet
Special Assistant for Federal/
State Relations

National Governors' Conference

Lanny Proffer
Director
Criminal Justice Project

Appendix V

SUGGESTED READING LIST PREPARED FOR SEMINAR PARTICIPANTS

SEMINAR ON PRIVACY
Washington, D. C. December 16-17, 1974

BIBLIOGRAPHIES

The following bibliographies represent comprehensive listings of reference materials dealing with personal privacy, record keeping, and data security. They have been used extensively in the preparation of this reading list.

Bibliography from: U. S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. *Federal Data Banks and Constitutional Rights: A Study of Data Systems on Individuals Maintained by Agencies of the United States Government*. Volume 6. Washington, U. S. Government Printing Office, 1974. 3513-3527 p.

Hunt, M. Kathleen and Rein Turn. *Privacy and Security in Databank Systems: An Annotated Bibliography, 1970-1973*. Santa Monica, the Rand Corporation, 1974. 166 p.

Bibliography from: *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*. U. S. Department of Health, Education, and Welfare. Washington, U. S. Government Printing Office, 1973. p. 298-330.

GENERAL REFERENCES

Aronoff, Stanley. "1984—Only 11 Years Away." *State Government*, v. 46, Spring 1973: 66–75.

Asserts that expanding private and public record keeping, assisted by computerization, constitutes a threat to the right of privacy. Because revenue sharing may make state and local governments the Nation's "primary information bounds", the author recommends that the states "take affirmative action to come to grips with the problems of records and data banks."

Association for Computing Machinery. Committee on Computers and Public Policy. "A Problem-List of Issues Concerning Computers and Public Policy: Report of the Committee." *Communications of the Association for Computing Machinery*, v. 17, Sept. 1974: 495-503.

Discusses some of the present and potential problems which arise at the intersection of computer utilization and various aspects of public policy. The issues reviewed include Computers and Privacy, Computers and Money, Information Services for Home Use, and Computers and Elections.

Association for Computing Machinery. Los Angeles Chapter. Ombudsman Committee. *Privacy in Information Systems: Phase I Report*. Los Angeles, Association for Computing Machinery, 1974. 23 p.

Report of the initial period of the committee's operation in which the committee sought to familiarize itself with published recommendations and pending legislation related to privacy. The committee's objectives are to study and make recommendations concerning the problems of conformance to proposed legislation and other recommendations for safeguarding privacy; to inform the public of its right to privacy; and to study the responsibility of data processing personnel in business to protect individuals' privacy in their job assignments. The committee is limiting its activities to areas of interest affecting the State of California.

Canada. Department of Communications and Department of Justice. *Privacy and Computers*. Ottawa, Information Canada, 1972. 236 p.

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.

Columbia Human Rights Law Review. Winter 1972: entire volume.

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. Tome, "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," and John P. Flannery, "Commercial Information Brokers."

Computer Security Handbook. Riverside, N. J.; McMillan Publishing Co., Inc., 1973.

" . . . Covers such risks as abuse of data, loss of data, physical hazards, equipment malfunction, software malfunction, and human error. Each of these areas is fully expored and detailed recommendations for implementation of protective measures are included."

"The Constitutional Right of Privacy: An Exami-

nation." *Northwestern University Law Review*, v. 69, May-June 1972: 263–301.

Reviews State and Federal court decisions dealing with constitutional protection of personal privacy.

Fried, Charles. "Privacy." *Yale Law Journal*, v. 77, Jan. 1968: 457-93.

Examines the foundations to the right of privacy. Discusses legal rules in the social context of privacy and the role of sanctions.

Goldstein, Robert C. *The Cost of Privacy: Operational and Financial Implications of Databank - Privacy Regulation*. Boston Honeywell Information Systems, 1975. 150 p.

Discusses a model for examining resource requirements and the cost impact of applying privacy regulations to personal data systems. The study also reports on a test of the model on six large data banks in both public and private organizations, including two systems operated by state law enforcement agencies.

IBM Corporation. *Data Security and Data Processing: Study of Specific Aspects of Data Security*. White Plains, N. Y., IBM Corporation, 1974. 1253 p.

A six-volume report of a study of specific aspects of data security funded by IBM and carried out at four study sites: the Massachusetts Institute of Technology, the State of Illinois, TRW Systems, Inc., and the IBM Federal Systems Center.

Illinois, State of, and IBM Corporation. Secure Automated Facility Environment Project. *The Elements and Economics of Information Privacy and Security*. Springfield, Illinois, Project SAFE, State of Illinois, 1974. 123 p. and appendices.

Publication resulting from the activities of Project SAFE established by the State of Illinois with the assistance of IBM Corporation, to develop safeguards for information systems. Contains a checklist of cost considerations. This overview from Project SAFE offers perspectives on technology, on costs and benefits, and on the social demands which government and industry must expect.

Levin, Eugene. "The Future Shock of Information Networks," *Astronautics and Aeronautics*, v. 11, Nov. 1973: 52-57.

States that ". . . we are at the threshold of a commitment to networks of computers.

"By 1976 it will be extremely difficult to incorporate the necessary controls in financial and government computer networks, and by 1980 it will probably no longer be possible to change events, only to preside over chaos."

Martin, James. *Security, Accuracy, and Privacy in Computer Systems*. Englewood Cliffs, N. J., Prentice Hall, Inc., 1973. 626 p.

A definitive text (including 90 pages of checklists and summaries) for security management.

"Measures to Protect Personal Privacy Increases at State Level." *Communications of the Association for Computing Machinery*, v. 16, Jan. 1973: 65-66.

Discusses two state actions favoring privacy as a fundamental right of citizens: one, the California voters' approval of the addition of privacy to the state constitution as an inalienable right; two, the Colorado Supreme Court decision that records of arrests without convictions could not be maintained.

Miller, Arthur R. *The Assault on Privacy: Computers, Data Banks, and Dossiers*. Ann Arbor, The University of Michigan Press, 1971. 334 p.

Discusses ". . . certain aspects of our increasingly electronic way of life . . . . Its aim is to explore some of the ways in which information technology is altering basic patterns in our daily life and to evaluate the responses being made by the law, government, industry, and other institutions to the new forms of data handling . . . ."

Parker, Donn B., Susan Nycum and S. Stephen Oura. *Computer Abuse*. Menlo Park, Calif., Stanford Research Institute, 1973. 131 p.

Considers computer abuse from the technical, legal, and sociological perspectives. It is the "first attempt to document and define the problem based on a typology of reported cases and investigation in detail of several of them." An appendix contains summaries of the cases (148) collected as a data base for continuing studies of computer abuse.

Parker, Richard B. "A Definition of Privacy," *Rutgers Law Review*, v. 27, 1974: 275-296.

Attempts "(1) to present and defend a definition of privacy which explains the close connection privacy has with the fourth amendment, and with some of the other amendments in the Bill of Rights; (2) to use the definition to clarify what privacy means in other legal and non-legal contexts; and, (3) to apply the definition to United States v. White to illustrate how and abstract definition of privacy can affect the analysis of a case."

Pennock, J. Roland and John W. Chapman, ed. *Privacy. Nomos XIII: Yearbook of the American Society for Political and Legal Philosophy*. New York, Atherton Press, 1971. 255 p.

A collection of papers which consider privacy from the perspectives of philosophy, political science, law, anthropology, politics, and sociology.

Ralston, Anthony G. "Computers and Democracy." *Computers and Automation*, v. 22, April 1973: 19–22, 40.

Discusses various aspects of the problem of balancing the use of computers for the good of society with the accompanying restrictions on personal freedom. The author concludes that "we must retain the hope that computers offer us while at the same time minimizing a threat we cannot eliminate."

Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems., U. S. Government Printing Office, 1973. 346 p. Also: Cambridge, Mass., Massachusetts Institute of Technology Press, 1973.

Report of an HEW-sponsored committee which 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; policy and practice relating to the issuance and use of Social Security numbers." This report discusses in depth the key issues identified, the findings of the Committee, and their specific recommendations and suggested action program.

Renninger, Clark R. and Dennis K. Branstad, ed. *Government Looks at Privacy and Security in Computer Systems*. Washington, National Bureau of Standards, U. S. Department of Commerce, 1974. 37p.

". . . Summarizes the proceedings of a conference held for the purpose of highlighting the needs and problems of Federal, State, and local governments in safeguarding individual privacy and protecting confidential data contained in computer systems from loss or misuse. The Conference was held at the National Bureau of Standards on November 19–20, 1973."

Renninger, Clark R., ed. *Approaches to Privacy and Security in Computer Systems*. Washington, National Bureau of Standards, U. S. Department of Commerce, 1974, 72 p.

". . . Summarizes and contains the proceedings of a conference held at the National Bureau of Standards on March 4–5, 1974, to continue the dialog in search of ways to protect confidential information in computer systems. Proposals are presented for meeting governmental needs in safegarding individual privacy and data confidentiality that were identified at a conference held in November 1973. Among the proposals are the enactment of privacy legislation, improved computer system architecture and access controls, information and security management guidelines and the development of a systematic, balanced approach to system security."

"Sweden's Data Act." *Computer Decisions*, Nov. 1973, p. 50–52.

Pertains to the act designed to protect personal information which became effective in Sweden on July 1, 1973. The Act is reproduced here.

Turn, Rein. *Privacy and Security in Personal Information Databank Systems*. Santa Monica, the Rand Corporation, 1974. 104 p.

Classifies databank systems on the basis of a number of data security related criteria. Such aspects of personal information as sensitivity and value are examined. A sensitivity scale and a personal information classification system are proposed. Using a game-theoretic model as the vehicle, costs and effectiveness of data protection, as well as costs of intrusion, are discussed. The report concludes with an analysis of implications of implementing the major components of total protective systems.

Ware, Willis H. *Data Banks, Privacy, and Society*. Report No. 5131. Santa Monica, the Rand Corporation, 1973. 11 p.

Discusses new dimensions to the problem of personal privacy added by the advent and use of computer technology with reference to information needs of society, the accessibility of personal information, and the potential for data linkages; contains suggestions for controlling the collection, dissemination, and use of personal data. The author concludes with a call to action in several areas: public education on the need for personal privacy, soliciting the support of consumer-oriented organizations for legislation, public participation in a debate on the implications of a fully-numbered society, and research on various aspects of personal privacy.

Warner, Malcolm and Michael Stone. *The Data Bank Society: Organizations, Computers, and Social Freedoms*. London, Unwin Brothers, Ltd., 1970. 244 p.

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.

Westin, Alan F. and Michael A. Baker. *Databanks in a Free Society: Computers, Record-Keeping and Privacy*. New York, Quadrangle Books, 1972. 552 p.

Report of the Project on Computer Databanks of the Computer Science and Engineering Board, National Academy of Sciences. The Project investigated "what the use of computers is actually doing to record-keeping processes in the United States, and what the growth of large-scale databanks, both manual and computerized, implies for the citizen's constitutional rights to privacy and due process."

Westin, Alan F., ed. *Information Technology in a Democracy*. Cambridge, Mass., Harvard University Press, 1971. 499 p.

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."

Westin, Alan F. *Privacy and Freedom*. New York, Atheneum Press, 1967. 487 p.

A seminal work on the implications of surveillance technologies for personal privacy.

Wheeler, Stanton, ed. *On Record: Files and Dossiers in American Life*. New York, Russell Sage Foundation, 1969. 499 p.

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.

Younger, K., Chairman. *Reports of the Committee on Privacy*. London, Her Majesty's Stationery Office, 1972. 350 pages.

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.

STATE AND LOCAL GOVERNMENT RECORDS ON INDIVIDUALS

California, State of. Intergovernmental Board on Electronic Data Processing. *Guidelines Establishing Requirements for Security and Confidentiality of Information Systems*. Sacramento, Calif., Documents Section, 1974. 74 p.

These guidelines alert management to the dangers posed by threats to security, confidentiality, and privacy and suggest preventive measures to minimize possibilities of loss. Each section, presented in checklist format, includes a bibliography.

Curran, William J., Eugene M. Laska, Honora Kaplan, and Rheta Bank. "Protection of Privacy and Confidentiality: Unique Law Protects Patient Records in a Multistate Psychiatric Information Systems," *Science*, v. 182, 1973: 797-802.

Describes the origins, purpose, and operations of the multistate information system, and existing procedures for maintaining confidentiality, including the special New York State protective statute.

"Integrated Municipal Information Systems: The USAC Approach — City Hall's Approaching Revolution in Service Delivery," *Nation's Cities*, Jan. 1972: 10-40.

Summary of a report prepared by the Federal Urban Information Systems Inter-Agency Committee. Describes the basic components of an IMIS and the steps required for their implementation.

Kauffman, Miles P. "Welfare and the Right to Privacy: Applicants Rights." *Res Ipsa Loquitur*, V. 25, Fall 1972: 107–113.

Contends that too often a citizen's right of privacy ceases to exist when he becomes a welfare recipient.

McNamara, Robert M., Jr. and Joyce R. Starr. "Confidentiality of Narcotic Addict Treatment Records: A Legal and Statistical Analysis." *Columbia Law Review*, v. 73, Dec. 1973: 1579 - 1612.

Examines the policies in handling treatment records of nearly two hundred narcotics treatment centers in the United States. Threats to records include overzealous law enforcement personnel and investigators for credit reporting bureaus. Legal mechanisms for improved protection of treatment records are analyzed.

National Assembly for Social Policy and Development, Inc. A *New Look at Confidentiality in Social Welfare Services*, New York, 1973. 14 p.

Presents guidelines and specific instructions to assist social welfare agencies in formulating appropriate policy for the protection of their clients' privacy. Agencies are urged to apply the recommendations of the HEW Secretary's Advisory Committee Report, as outlined here, to both computerized and manual files.

National Association for State Information Systems. *Information Systems Technology in State Governments 1973 NASIS Report*. (1974. Available from the Council of State Governments, Iron Works Pike, Lexington, Ky., 40505) 60. p. and appendices.

"Information was sought for the first time on some of the basic problems relating to security and privacy. The security questions had to do with physical and data security procedures. Privacy questions were aimed at obtaining an overview of the status of legislation and estimates of public concern."

Noble, John H,. Jr. "Protecting the Public's Privacy in Computerized Health and Welfare Information Systems." *Social Work*, v. 16, Jan. 1971: 35-41.

Discusses the impact of automated record keeping on the traditional practices of social work and health professionals. Suggests guidelines by which to judge proposals to automate existing information systems and urges support of legislation to regulate all computerized databanks.

"Public Access to Government-held Computerized Information." *Northwestern University Law Review*, v. 68. May-June 1973: 433-462.

Comment reviews existing literature on computers and privacy, documents ways in which government computer facilities can safeguard privacy, and evaluates chances of success for such safeguards.

Rioux, J. William and Stuart A. Sandow. *Children, Parents, and School Records*. Columbia, Md., National Committee for Citizens in Education, 1974. 313 p.

Advocates reform of school record-keeping practices to assure the privacy and due process rights of students. Contains general information, readings, relevant data about each state, examples to substantiate the authors' position, and suggestions for action.

Stallings, C. Wayne. "Local Information Policy: Confidentiality and Public Access." *Public Administration Review*, v. 34, May-June 1974: 197-204.

Outlines a model policy for local governments that protects privacy while assuring legitimate public access to government records. Presents a scheme for classifying various types of information and specifying appropriate degrees of access to each type, and discusses an organizational structure to regulate such access. (Summary of a larger report prepared for the Charlotte Integrated Municipal Information Project).

Steinberg, Joseph. "Some Aspects of Statistical Data Linkage for Individuals." *In Data Bases, Computers, and the Social Sciences*. New York, John Wiley and Sons, Intersciences Division, 1970. p. 238 - 251.

Examines evidence of concern by the Social Security Administration regarding the possible role of the Social Security Number in facilitating invasions of privacy. Discusses the release of Social Security data for research purposes, violations of statistical confidentiality, and refusal of the Social Security Administration to cooperate with proposed use of the SSN by other agencies.

U. S. Congress. House. Committee on Government Operations. Foreign Operations and Government Information Subcommittee. *Access to Records*. Hearings, 93d Congress, 2d session, on H. R. 12206 and Related Bills. Washington, U. S. Government Printing Office, 1974. 338 p.

"H. R. 12206 and related bills, to amend Title 5, United States Code, to provide that persons be apprised of records concerning them which are maintained by government agencies." Hearings held Feb. 19, 26, April 30, and May 16, 1974.

U. S. Congress. Senate. Committee on Government Operations, Ad Hoc Subcommittee on Privacy and Information Systems. Committee on the Judiciary. Subcommittee on Constitutional Rights. *Privacy: The Collection, Use, and Compterization of Personal Data*. Joint Hearings, 93d Congress, 2d session, on S. 3418, S. 3633, S. 3116, S. 2810, S. 2542. June 18-20, 1974. Parts I and II, Washington, U. S. Government Printing Office, 1974. 2335 p.

Hearings on a series of bills proposing controls over government and commercial databanks in order to safeguard the privacy rights of individuals who are the subjects of these information systems.

Zastrow, Charles. "The Status of Communitywide Social Data Banks." *Welfare in Review*, v. 10, Mar. - Apr. 1972: 32-36.

Findings from a study of the feasibility of a community-wide automated social information center in Dane County (Madison), Wisconsin conducted by its Social Planning Agency. See discussions of confidentiality and access to data.

PUBLIC EMPLOYEES' RECORDS

"Application of the Constitutional Privacy Right to Exclusions and Dismissals from Public Employment." *Duke Law Journal*, Dec. 1973: 1037-1062.

Gaillard, Frye. "Polygraphs and Privacy." *The Progressive*, Sept. 1974: 43-46.

Discusses the increasing use of the polygraph by business establishments to test applicants'/employees' honesty, usually for one of three purposes: (1) pre-employment screening, (2) a periodic sampling of workers to test basic honesty, loyalty, and adherence to company policy, and (3) specific tests directed to solving particular thefts or irregularities.

Miller, Herbert S. *The Closed Door: The Effect of a Criminal Record on Employment with State and Local Public Agencies.* Washington, Institute of Criminal Law and Procedure, Georgetown University Law Center, 1972. 252 p.

Indicates that an arrest record even without conviction is a substantial handicap. Despite protective laws, juvenile records are not confidentiality maintained; arrest records are often incomplete; and arrest records are widely circulated via the FBI. The recommended solutions are an Equal Employment Opportunity Commission order pending the enactment of federal legislation.

U. S. Congress. House. Committee on Post Office and Civil Service. Subcommittee on Retirement and Employee Benefits. *Right to Privacy of Federal Employees.* Hearings, 93d Congress, 1st and 2d sessions, on H. R. 1281 and related bills. Washington, U. S. Government Printing Office, 1974. 378 p.

"H. R. 1281 and related bills, to protect the civilian employees of the Executive Branch of the United States Government in the enjoyment of their constitutional rights and to prevent unwarranted governmental invasions of their privacy." Hearings held May 14 and 15, June 4, 1973 and April 24, August 8, 1974. Many of the concepts discussed in these hearings are equally applicable to the privacy rights of employees of state and local governments.

Walsh, Timothy J. "Background Information Use Limited by New Law." *Industrial Security*, April 1971: 4–12.

Summarizes restrictions on the use of background investigations for screening prospective employees contained in the Fair Credit Reporting Act and the Gregory vs. Litton decision.

CRIMINAL JUSTICE INFORMATION

Gallati, Robert R. J. "State Criminal Justice Information Systems." *AFIPS Conference Proceedings*, v. 39, 1971: 303–308.

Traces the development of the New York State Identification and Intelligence System as a case study of a model criminal identification bureau. Outlines several major problems encountered, e.g., need for autonomy, difficulties in data conversion, and state-of-the-art technology in automated identification.

Gates, Andrew L. "Arrest Records—Protecting the Innocent." *Tulane Law Review*, v. 48, April 1974: 629–648.

Longton, Paul A. "Constitutional Law—Maintenance and Dissemination of Records of Arrest Versus the Right to Privacy." Wayne Law Review, v. 17, July-Aug. 1971.

MacDonald, Malcolm E. "Computer Support for the Courts—A Case for Cautious Optimism." *Judicature*, v. 57, Aug.-Sept. 1973: 52–55.

Reviews some successful applications of computer technology to court administration, such as jury selection, criminal case docketing, scheduling, etc. Stresses the need to proceed carefully with innovative applications, which should reflect appropriate law and procedure, court requirements, and security standards.

National Advisory Commission on Criminal Justice Standards and Goals. *Criminal Justice Systems.* Washington, U. S. Government Printing Office, 1973.

Presents extensive and detailed criteria for criminal justice systems, with explanatory comments. These sixty-eight standards fall into four categories—planning, information systems, education, and legislation—and apply variously to the local, state and federal levels.

National Council of Juvenile Court Judges. *Computer Applications in the Juvenile Justice System: Proceedings of the National Symposium on Computer Applications in the Juvenile Justice System,* Atlanta, Georgia, Dec. 6–8, 1973. (Reno, Nevada, University of Nevada) 1974. 248 p.

Describes the impact of computers on different aspects of juvenile justice administration. Includes papers by Melvin F. Bockelman and Malcolm E. MacDonald on privacy and security considerations.

New York, State of. 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.

Project SEARCH, i.e., System for Electronic Analysis and Retrieval of Criminal Histories. (A combined effort, initialed in 1969 by the Law Enforcement Assistance Administration and several states, to develop a prototype computerized criminal information system. Specialized committees, merging expertise from all parts of the country, wrote the following reports. They were published by Project SEARCH, which recently shed its government sponsorship. Its work continues under the auspices of SEARCH Group, Inc., a non-profit research organization headquartered in Sacramento, California.)

Computer Hardware and Software Considerations. (Technical Memorandum No. 6) Jan. 1974. 40 p.

Design of a Model State Identification Bureau. (Technical Report No. 8) Nov. 1973. 143 p. and appendix.

Design of a Standardized Crime Reporting System. (Technical Report No. 9) Dec. 1973. 140 p.

Designing Statewide Criminal Justice Statistics Systems—An Examination of the Five-State Implementation. (Technical Report No. 5) Dec. 1972. 137 p.

Designing Statewide Criminal Justice Statistics Systems—The Demonstration Prototype. (Technical Report No. 3) Nov. 1970. 60 p. and appendix.

Model Administrative Regulations For Criminal Offender Record Information. (Technical Memorandum No. 4) March 1973. 67 p.

A Model State Act For Criminal Offender Record Information. (Technical Memorandum No. 3) May 1971. 46 p.

Preliminary Requirements Analysis For Criminal Justice—Law Enforcement Telecommunications. (Technical Memorandum No. 7) Jan. 1974. 170 p.

Project SEARCH Security and Privacy Publications. (Technical Report No. 2, Technical Memorandum No. 3, and Technical Memorandum No. 4) May 1973. (various pagings.)

Security and Privacy Considerations in Criminal History Information Systems. (Technical Report No. 2) July 1970. 57 p.

Terminal Users Agreement for CCH and Other Criminal Justice Information. (Technical Memorandum No. 5) Nov. 1973. 13 p.

Shappley, William L. "Branded: Arrest Records of the Unconvicted." *Mississippi Law Journal*, v. 44, 1973: 928–946.

Discusses "individual rights of privacy as constitutionally guaranteed and as balanced against the public necessity for retention of arrest-record data." Reviews the statutory approach of California, Connecticut, Illinois, and New York. Pertinent judicial decisions, and the current Mississippi position.

U. S. Congress. House. Committee on the Judiciary. Subcommittee No. 4. *Security and Privacy of Criminal Arrest Records.* Hearings, 92d Congress, 2d session, on H. R. 13315. Washington, U. S. Government Printing Office, 1972. 520 p.

Hearings held March 16, 22, 23, April 13, 26, 1972. Explores methods of safeguarding, simultaneously, individual privacy and the needs of law enforcement officials.

U. S. Congress. House. Committee on the Judiciary Subcommittee on Civil Rights and Constitutional Rights. *Dissemination of Criminal Justice Information.* Hearings, 93d Congress, on H. R. 188, H. R. 9783, H. R. 12574, H. R. 12575. Washington: U. S. Government Printing Office, 1974. 586 p.

Hearings held July 26, September 26, and October 11, 1973; February 26, 28, March 5, 28, and April 3, 1974.

U. S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. *Criminal Justice Data Banks.* Hearings, 93d Congress, 2d session on S. 2542, S. 2810, S. 2963, and S. 2964. March 5–7; 12–14, 1974. 2 Vols. Washington, U. S. Government Printing Office, 1974. 1149 p.

Examines the need for legislation "to protect the privacy and reputations of persons whose names appear in criminal justice data banks" in light of law enforcement practices and requirements.

U. S. General Accounting Office. Comptroller General of the United States. *How Criminal Justice Agencies Subcommittee on Constitutional Rights, Committee on the Judiciary, United States Senate.* Washington, General Accounting Office, 1974. 70 p.

Summarizes findings based on an analysis of a random sample of requests made by agencies in California, Florida, Massachusetts, and by Federal agencies, to the Federal Bureau of Investigation (FBI) and appropriate state agencies.

Wormeli, Park K. "The SEARCH For Automated Justice." *Datamation,* v. 17, June 15, 1971: 32–35

Discusses the multi-state Project SEARCH (System for Electronic Analysis and Retrieval of Criminal Histories). This article, by the Project coordinator, details the objectives, system concept, procedures, progress, and status of the program.

RECORDS ON CONSUMERS

American Bankers Association. *Report of the Automated Clearing House Task Force.* Washington, American Bankers Association, 1974. 94 p.

An effort to establish industrywide standards for the electronic transfer of funds nation-wide. The American Banking Association report recommends that a national automated clearinghouse association be established for continued analysis of problems and opportunities; that automated clearinghouses be established in each region of the U. S.; that action be taken to increase general understanding of the concept to insure full development; and that all parties concerned step up education and marketing research efforts.

Foer, Albert A. "The Personal Information Market: An Examination of the Scope and Impact of the Fair Credit Reporting Act." *Loyola Law Students Consumer Journal,* v. II, 1974: 37–138.

Discusses a study of the personal information market in the Chicago area to assess the impact of the Fair Credit Reporting Act. The new law is evaluated in terms of its "ability to cope with seven particular abuses" present prior to passage of the FCRA. A final section sets out and weighs various suggested strategies for reform.

"Government Access to Bank Records." Note. *Yale Law Journal,* v. 83, 1974: 1439–1474.

". . . Isolates the problem of government access to one type of third party data: checking account records maintained by commercial banks. It is argued that, given the purposes of the Fourth Amendment and the changes which have taken place in the nature of property and privacy, individuals should be able to contest an unreasonable search and seizure of their bank records . . . Maintains that banks ordinarily lack authority to consent to a government search of depositors' records.

Hendrickson, Robert. *The Cashless Society.* New York, Dodd, Mead & Co., 1972.

A discussion of the increasing reliance on credit systems and the implications for individual freedom.

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.

Parker, Suzanne. *The Electronic Funds Transfer System.* Washington, Library of Congress, Congressional Research Service, 1974. 18 p.

". . . Discusses the development of the system to date as well as those changes which are visualized. In addition, the possible impact of the system on various segments of the economy will be covered. Finally, discussion of the proposals relating to how the system should be implemented and controlled will be included."

Prism: The Socioeconomic Magazine of the American Medical Association, v. 2, June 1974: entire issue.

Devoted to a comprehensive report on privacy and confidentiality. The editors have attempted to set the subject of privacy in its social context, focusing on special medical implications of privacy. The issue includes articles by such legal scholars as Senator Sam J. Ervin, Jr., Arthur R. Miller, and Alan F. Westin, as well as such physician contributors as Alfred M. Freedman, Carmault B. Jackson, and Ralph Crawshaw.

"Protecting the Subjects of Credit Reports." Note. *Yale Law Journal,* v. 80, April 1971: 1035–1069.

". . . Identifies the injuries and costs of credit reporting and suggests that enterprise liability and further legislation are required for the protection of the consumer." This article appeared shortly after the enactment of the Fair Credit Reporting Act.

Rule, James B. *Private Lives and Public Surveillance: Social Control in the Computer Age.* New York, Schocken Books, Inc., 1974. 382 p.

Discusses the use of personal information as a means of social control. The record-keeping activities involved in police record systems, vehicle and driver licensing, National Insurance in England, and consumer credit and the Bankamericard systems in the United States are analyzed.

Sackman, Harold and Norman Nie, ed. *The Information Utility and Social Choice.* Montvale, N. J., AFIPS Press, 1970. 299 p.

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.

Stanley, David T. and Marjorie Girth, ed. *Bankruptcy: Problem, Process, Reform.* Washington, The Brookings Institution, 1971. 270 p.

Reviews current procedures in bankruptcy in the United States (which relate to issues of consumer record-keeping). . . . "deals with the economic, legal, and personal aspects of the subject, but its main emphasis is on bankruptcy as a governmental process—on its institutions, personnel, procedures, and financing.

Stern, Laurence C. "Medical Information Bureau: The Life Insurer's Databank." *Rutgers Journal of Computers and the Law,* v. 4, No. 1, 1974: 1–41.

Reviews the background and operation of the Medical Information Bureau, an association of life insurance companies, which enables member companies to exchange underwriting and claims information about life insurance applicants and claimants. The author discusses the Bureau's relationship to the requirements of the Fair Credit Reporting Act and other consumer privacy protection issues.

U. S. Congress. House. Committee on Government Operations. Foreign Operations and Government Information Subcommittee. *Sale or Distribution of Mailing Lists by Federal Agencies.* Hearings, 92d Congress, 2d session, on H. R. 8903 and Related Bills. June 13 and 15, 1972. Washington: U. S. Government Printing Office, 1972. 362 p.

Hearings on proposals to amend the Freedom of Information Act to eliminate the dissemination of Government-prepared lists for commercial or solicitation use. Raises issues which would apply to the use and distribution of mailing lists by other public agencies and private organizations.

U. S. Congress. Senate. Committee on Banking, Housing and Urban Affairs. Subcommittee on Consumer Credit. *Fair Credit Reporting Act—1973:* Hearings, 93d Congress, 1st session, on S. 2360. October 1–5, 1973. Washington, U. S. Government Printing Office, 1973. 993 p.

Hearings on proposed amendment of the Fair Credit Reporting Act. Review of the administration of the Act to determine if additional consumer safeguards are needed.

U. S. Congress. Senate. Committee on Banking, Housing and Urban Affairs. Subcommittee on Consumer Credit. *Credit Reporting Abuses.* Hearings, 93d Congress, 2d session on amending the Fair Credit Reporting Act. February 5, 1974. Washington: U. S. Government Printing Office, 1974. 54 p.

Hearings on abuse in the credit reporting industry, prompted by the Subcommittee's decision to table S. 2360 in November 1973.

Urban Planning Aid, Inc. The Media Project. *The Cable Book: Community Television for Massachusetts?* Cambridge, Mass., Urban Planning Aid, Inc., 1974. 106 p.

A handbook for ". . . groups who are trying to figure out what it's (cable television) all about and what it's going to mean to them and their communities." Chapter 5 deals with the privacy impact of cable television.

Westermeier, John T., Jr. "The Privacy Side of the Credit Card." *American University Law Review,* v. 23, Fall 1973: 183–207.

". . . Examines credit card use in light of the developing right of privacy. The focus will be on the loss of privacy that results from excluding the cardholder from the decisions concerning the exchange of personal information that is collected and maintained in the operation of the credit card system."

Wetterhus, Alan. "The Cashless, Checkless Society: On Its Way?" *Computers and Automation,* v. 21, Nov. 1972: 14–15, 17.

Discusses the utilization of computer systems to transfer funds between accounts via electronic impulses, e.g., directly from a customer's bank account to a retailer from whom he is making a purchase. Some bankers have expressed concern about the practicality and profitability of these systems and questions exist about customer acceptance and invasion of personal privacy. However, pilot studies are under way in various locations as part of banks' growing recognition of a need to become full financial service institutions.

Willis, Donald S. "Who Knows You: A Look at Commercial Data Banks." *Computers and Automation,* v. 22, March 1973: 18–21.

Discusses some common commercial data banks (credit, investigative, sales prospects) with respect to the threat they pose to personal privacy.

THE DOSSIER SOCIETY †

Arthur R. Miller *

IN RECENT YEARS there has been a growing public awareness of the effects certain data-gathering activities and applications of information technology may have on individual and commercial privacy. At times the debate has been conducted in emotional terms. For example, many people, myself included I must confess, have voiced the fear that the computer, with its insatiable appetite for information, its image of infallibility, and its inability to forget anything that has been put into it, may become the heart of a surveillance system that will turn society into a transparent world in which our home, our finances, and our associations are bared to the most casual observer.[1]

A brief recital of some of the blessings and blasphemies of the new technology makes the computer-privacy dilemma abundantly clear. In various medical centers, doctors are using computers to monitor physiological changes in the bodies of heart patients in the hope of isolating those alterations in body chemistry that precede a heart attack. The quest, of course, is to provide an "early warning system" so that treatment is not delayed until the actual heart attack has rendered the patient moribund for all practical purposes. Other plans include providing everyone a number at birth to identify them for tax, banking, education, social security, and draft purposes. This would be done in conjunction with the computerization of a wide range of records. The goal is to eliminate much of the existing multiplicity in record-keeping, and at the same time expedite the business of society. Long range goals include developing a checkless, cashless economy, improving the informational bases available for rational planning, providing better services to people, and promoting the equitable allocation of society's resources. We may even see the day when if a person falls ill while away from home, a local doctor can use this identification number to retrieve the patient's medical history and drug reactions from a central data bank.

On the opposite side of the ledger, the same electronic sensors that can warn us of an impending heart attack might be used to locate us, track our movements, and measure our emotions and thoughts. Experiments already are underway in the field of telemetering and significant breakthroughs are on the horizon. Similarly, the identification number given us at birth might become a leash around our necks and make us the object of constant monitoring, making credible the fear of the much fabled womb-to-tomb dossier. Finally, the administrative conveniences provided by the high degree of information centralization made possible through the widescale use of computers gives those who control the recordation and preservation of personal data a degree of power over us that is unprecedented and subject to abuse.[2]

Close scrutiny and evaluation of the implications of data technology and information systems on individual privacy are especially appropriate at this time because of the clarion in all quarters for the establishment of governmental and private data centers. For example, the United States Office of Education is supporting a migrant worker children data bank, the Department of Housing and Urban Development is sponsoring computerized municipal information systems and building files on housing loan applicants (with particular attention given to those who are ineligible), and President Nixon's welfare reform proposal (the Family Assistance and Manpower Training Acts) will give the Department of Health, Education and Welfare authority to exchange individualized data with state welfare agencies and lead to the establishment of a national job applicant data bank. In other areas, we are seeing the emergence of criminal intelligence data centers, such as the Federal Bureau of Investigation's National Crime Information Center (NCIC), and computer based credit rating services. As we look to the future, there is no doubt that the hypnotic attraction of digital record-keeping will continue to envelope our universities, corporations, hospitals, and banks.

Indeed, I believe that Americans today are scrutinized, watched, counted, recorded, and questioned by more governmental agencies, social scientists, and law enforcement officials than at any other time in our history. Whether he knows it or not, each time a citizen files a tax return, applies for life insurance or a credit card, seeks government benefits, or interviews for a job, a dossier is opened under his name and his informational profile is sketched. It has now reached the point at which whenever we travel on a commercial airline, reserve a room at one of the national hotel chains, or rent a car we are likely to leave distinctive tracks in the memory of a computer—tracks that can tell a great deal about our activities, habits, and associations when collated and analyzed. Few people seem to appreciate the fact that modern technology is capable of monitoring, centralizing, and evaluating these electronic entries—no matter how numerous and scattered they may be.

Federal agencies and private companies are using computers and microfilm technology to collect, store, and exchange information about the activities of private citizens to an astounding degree. Rarely does a week go by without the existence of some new data bank being disclosed. During the past year we have read of the Department of Housing and Urban Development's Adverse Information File, the National Science Foundation's data bank on scientists, the Customs Bureau's computerized data bank on "suspects," the Civil Service Commission's "investigative" and "security" files, the Justice Department's intelligence bank run by that organization's civil disturbance group, the fact that files on 2.6 million individuals are maintained by the Department of Transportation's National Driver Register Service, the Secret Service's dossiers on "undesirables," "activists," and "malcontents," and the surveillance activities of the United States Army. These are only some of the federal government's data banks that have been brought to light; even now only the tip of the iceberg may be visible.

By and large, these data gathering activities are well intended efforts to achieve socially desirable objectives. For example, in the law enforcement field, file-building is necessary to combat organized crime and restore "Law and Order." In a similar vein, the FBI and the Army can justify their intelligence activities in terms of combating subversion or quelling campus disruptions and riots in our urbans centers by knowing who to watch or seize in times of strife. As to the information activities of credit grantors, private investigators, and insurance companies, which involve considerable snooping into an individual's private life, it simply is good business to know as much as possible about a man before you lend him money, employ him, or insure his life.

But there is a negative side to these mushrooming data banks—particularly those that bear the imprimatur of a governmental organization. Consider the information practices of the United States Army. Early last year it was revealed that for some time Army intelligence units were systematically keeping watch on the *lawful* political activity of a number of groups and preparing "incident" reports and dossiers on individuals engaging in a wide range of *legal* protests. It must be emphasized that this monitoring not only covered society's "crazies" but included such nonviolent organizations as the NAACP, the ACLU, the Southern Christian Leadership Conference, and the Women Strike for Peace, and allegedly extended to newsmen, congressmen, and a former governor who is now a federal judge.

Although there is considerable justification for certain types of information collection that are directly relevant to the Army's duties, the development of dossiers on people pursuing lawful social and political activities bears little relationship to the function of the military—even to its function during periods of social unrest. This is especially true when many of those being scrutinized are extremely unlikely to be involved in riotous conduct, and the

† These remarks were originally delivered as a lecture in the Privacy and the Law series at the University of Illinois College of Law, March 25, 1971. Reprinted with permission from *University of Illinois Law Forum*, Vol. 1971 No. 2, pp. 154–167.

* Professor of Law, Harvard University. The author has more fully explored the subject matter of his address in A. Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers* (1971), *and* Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 Mich. L. Rev. 1089 (1969).

[1] Miller, *The National Data Center and Personal Privacy*, *The Atlantic*, Nov. 1967, at 53-57.

[2] Dombrowski v. Pfister, 380 U.S. 479, 487, 85 S. Ct. 1116, 1121 (1965).

selection of suspects seems to be governed by an incredibly simplistic these-are-the-good-guys-and-those-are-the-bad-guys approach. Not only is the Army's file-building difficult to justify, but it appears to have been undertaken without sufficient appreciation of the fact that the creation and exposure of dossiers on people who are politically active could deter them from exercising their right to assemble, speak freely, or petition the government.

The development of a number of other information systems in the law enforcement arena magnifies both the threat to personal privacy and the potential "chilling effect" of informational surveillance. The FBI's constantly expanding National Crime Information Center (prominently featured on the television series, "The FBI") provides state and city police forces with immediate access to computerized files on many people. Although it currently only contains data on fugitives and stolen property, plans are being formulated to add arrest records and other types of information to the FBI system. Moreover, NCIC is the keystone of an emerging information network that will tie together the nation's law enforcement information centers. By the end of 1969, the Crime Information Center reportedly was already exchanging data with state and local police agencies in every state except Alaska. State and local law enforcement surveillance systems also are becoming increasingly sophisticated—several with the aid of funding from the federal government under the Law Enforcement Assistance Administration program. New York already has the essential features of a network built around a single computer center designed to store information for state and local agencies and permit them to retrieve data through terminals placed throughout the state. An Ohio system allows 38 agencies to share its computerized information and is connected both to NCIC and the Ohio State Highway Patrol computer center; plans are underway to tie it to comparable systems in Kentucky and Indiana.

If a citizen knows that his conduct and associations are being put "on file," and he knows that there is some possibility that the information might be used to harass or injure him, he may become more concerned about the possible content of that file and less willing to "stick his neck out" in pursuit of his constitutional rights. The effect may be (to paraphrase a thought expressed by Justice Brennan in an analogous context) to encourage Americans to keep their mouths shut on all occasions.[3]

If we really take our constitutional guarantees seriously, we cannot afford to stand by and allow them to be debilitated by this type of coercion. Claims of governmental efficiency or the war against crime and subversion must not be allowed to justify every demand for gathering personal data. Because of the potential development of a "record prison" mentality, no one should be surprised if some suggest that today's surveillance efforts contain the seeds of the much dreaded police state or a return to McCarthyism. Nor is it sufficient that governmental agencies assure us that surveillance and file-building are not being engaged in for repressive purposes. Nineteen eighty-four is a state of mind; for many people, the appearance of repression may have the impact of reality.

To prevent any doubt on the point, I personally do not oppose information systems or computerization of data. It strikes me as foolish to prevent the use of a modern technology to carry out important governmental and nongovernmental operations simply because it might be abused. This is especially true in our complex, urbanized society and mass economy, which desperately need data for sound national planning. We cannot turn the hands on the clock back. But this does not justify inaction. Even now we should recognize the strong similarity between the difficulties that gave rise to the multi-faceted regulation of airlines, automobiles, railroads, radio, and television and the problems that already are generating pressure for the comprehensive regulation of data banks and computer communications.

What is necessary at this time is the development of a framework for the protection of the public and the superimposition of that framework on information practices at an early date to minimize misuse of an otherwise socially desirable instrument. The problem of striking a balance between democracy and technology has been a frequent and manageable chore in the past and the nation's policy makers should not shrink from the task in this context.

Let us turn now to the particular tensions between contemporary data activities and privacy. Until recently, informational privacy has been relatively easy to protect for a number of reasons: (1) large quantities of information about individuals have not been available; (2) the available information generally has been decentralized; (3) the available information has been relatively superficial; (4) access to information has been difficult to secure; (5) people in a highly mobile society are difficult to keep track of; and (6) most people were unable to interpret and infer revealing information from data.

But these protections were part of a bygone era and are alien to our technologically based society. The testimony elicited before several committees of the United States Congress that have held hearings on privacy presents an astounding, and disheartening, panorama of the ways in which the intruders in our society, aided by the fruits of modern science, have destroyed many of these traditional bastions of privacy.[4] Revelations concerning the widespread use of spike and parabolic microphones, a variety of gadgets for electronic eavesdroping, cameras equipped with modern optical devices that enable photographs to be taken at a distance and under adverse weather or light conditions, demonstrate that we do not necessarily enjoy physical privacy in our homes or offices, on the street, or while taking communion with a martini.

Now, ever increasing resort to the computer, laser technology, and microminiaturization techniques has begun to erode our informational privacy. Because the new technology makes it possible to integrate personal information from a variety of sources, solicitation lists increasingly are becoming the product of wide-ranging file investigations into the backgrounds and finances of prospective customers.[5] Personal information can be used for commercial purposes, such as generating a list of consumers with certain characteristics. *Reader's Digest* reportedly has used computer technology to produce a mailing list consisting of its subscribers' neighbors. "The approach had a kind of 'all the neighbors are doing it' quality," said one commentator. "But, more significantly, the individual was pleased that the *Reader's Digest* knew him and could relate him to others on his block."[6]

It should be evident to all that we live in an increasingly information based society. For example, ever since the federal government entered into the taxation and social welfare spheres, greater quantities of information have been sought from citizens and recorded. Moreover, in recent years access to governmental or institutional largesse has increasingly depended upon a willingness to divulge private information. As recording processes have become cheaper and more efficient, this data collection trend has intensified and been accompanied by a predilection toward centralization and collation. The effect is something akin to Parkinson's Law. As capacity for information handling has increased, there has been a tendency to engage in more extensive manipulation and analysis of recorded data, which, in turn, has motivated the collection of data pertaining to a larger number of variables. The availability of electronic data storage and retrieval has accelerated this pattern, as is made evident by comparing the questions on a 1970 in-

[3] Lopez v. United States, 373 U.S. 427, 450, 83 S. Ct. 1381, 1393-94 (1963) (dissenting opinion).

[4] *See generally Hearings on Federal Data Banks and the Bill of Rights Before the Subcomm. on Constitutional Rights of the Comm. on the Judiciary*, 91st Cong., 1 Sess. (1971); *Hearings on Commercial Credit Bureaus Before a Subcomm. of the House Comm. on Government Operations*, 90th Cong., 2d Sess. (1968); *Hearings on Computer Privacy Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary*, 90th Cong., 2d Sess. (1968); *Hearings on the Coordination and Integration of Government Statistical Programs Before the Subcomm. on Economic Statisics of the Joint Economic Comm.*, 90th Cong., 1st Sess. (1967); *Hearings on the Computer and Invasion of Privacy Before a Subcomm. of the House Comm. on Government Operations*, 89th Cong., 2d Sess. (1966).

[5] *See* A. Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers* 79–85 (1971).

[6] N.Y. Times, July 30, 1968, at 41, col. 1.

come tax form with those on a 1960 form and the significantly greater incidence of intrusive governmental, industrial, and academic questionnaires. It is now feasible to execute and evaluate these inquiries because of the availability of machine processing.

I think it is reasonable to assume that one consequence of the advent of data centers and increased computer capacity is that many governmental and private information gathering agencies will go beyond current levels of inquiry and begin to ask more complex, probing, and sensitive questions—perhaps into such subjects as associations with other people, location and activity at different points of time and space, medical history, and attitudes toward various institutions and persons.

There are additional risks lurking in the ever-increasing reliance on recorded information and third-party evaluations of a person's past performance. As information cumulates, the contents of an individual's computerized dossier appear more and more impressive, despite the "softness" of much of the data, and impart to the user a heightened sense of reliability. Coupled with the myth of computer infallibility, this will make it less likely that an independent evaluation will be made or that verification of the data will be sought. We are beginning to see more and more adherence to the file in the credit granting, insurance, educational, and employment fields.

I know a talented young lady who was unable to gain employment for some time following graduation from college because potential employers were wary of an entry in her university file that she became aware of after many painful experiences. It said: "Melinda's mother is emotionally unstable." It turned out that this comment had been made by the girl's sixth grade teacher, who was neither a psychiatrist nor a psychologist and had only met the child's mother casually. Yet this damaging entry had been preserved and had followed Melinda for 15 years without anyone questioning either its retention or its reliability. Thus, not surprisingly, many people have come to feel that their success or failure in life ultimately may turn on what other people put in their file and an unknown programmer's ability—or inability—to evaluate, process, and interrelate information. Moverover, as things now stand, a computerized file has a certain indelible quality—an adversity not to be overcome with time, absent an electronic eraser and a compassionate soul willing to use it.

The centralization of information from widely divergent sources also creates serious problems of information accuracy. I am not really speaking of the literal accuracy of the input and what is recorded in the system, although that itself becomes a more serious problem as we increase the content of dossiers and magnify the possibility of error. Rather, I am concerned about the risks of using data out of context. Information can be entirely accurate and sufficient in one context and wholly incomplete and misleading in another. Consider the fact that computerization has made it convenient to rate an employee's efficiency and personal habits according to concise, conclusory categories such as "excellent," "fair," or "good" and that organizations often lack common traditions of appraising or interpreting performance. Anyone not conversant with military minds and mores might be misled by a rating of "superhuman" by the United States Army, which might be equivalent to a rating of "qualified" in a more demanding organization.

The problem of contextual accuracy can be illustrated in terms of one of the most dangerous types of personal information currently maintained—the unexplained and incomplete arrest record. Is it likely that a citizen whose file contains an entry "arrested, 6/1/42; convicted felony, 1/6/43; sentenced, three years Leavenworth" will be given government employment or be accorded some of the other societal amenities of modern life? Yet our subject simply may have been a conscientious objector during the Second World War. Consider the potential effect of a computer entry "arrested, criminal trespass; sentenced, six months." Without more, how will the user know that our computerized man was simply demonstrating for equal employment in the North or desegregation in the South in the 1950's and was convicted under a statute that was overturned on appeal as an unconsititutional restraint on free speech?

In an era of great social activism on the part of the young, with counterpoint demands from others for "Law and Order," arrests are bound to increase. But many of them will be of a strikingly different character than what has been typical in the past. It is now common for hundreds of college demonstrators or black militants to be arrested in connection with one incident. Using recent experience as a guide, only a small fraction of the group will be prosecuted, and an even smaller number convicted. All of them, however, will have arrest records. Unless these records show disposition, their circulation may have an improperly prejudicial effect.

It also seems evident that the desirability of getting at a data center's enormous store of information may well offset the difficulties of gaining access to its computerized files and deciphering them, which are occasionally offered as reasons why machine readable information is inherently more secure than manually stored data. Even if we assume that the cost of securing access to computerized "dirt" is higher than the cost of dredging out the "dirt" in a more traditional form of record, the centralized quality and compactness of a computerized dossier creates an incentive to invade it because the payoff for doing so successfully may be sufficiently large that the cost per unit of computerized "dirt" acutally will prove to be lower than the cost per unit of uncomputerized "dirt."

It should not be forgotten that the risks to privacy created by data centers lie not only in abuse of the system by those who desire to injure others or who can obtain some personal advantage by doing so. There is a legitimate fear of over-centalizing individualized information and then proliferating the number of people who, by having access to it, also have the capacity to inflict damage through negligence, sloppiness, and sheer stupidity. Unthinking people are as capable of injuring others by unintentionally rendering a record inaccurate, losing it, or disseminating its contents to unauthorized people, as are people acting out of malice or for personal aggrandizement.

What then is the solution? As an initial matter, one would hope that good judgment and self-regulation on the part of the information gathering and using communities would suffice. Those who handle individualized data—whether it be in the context of financial profiles in a credit bureau, student records in a school system, medical files in a hospital, welfare lists in a governmental agency, or personnel data in a large corporation—have an obligation to guard the privacy of the human beings whose lives are reflected in those dossiers. But we must also come to grips with a basic fact of life concerning computerized information systems. The only completely effective guardian of individual privacy is the imposition of *strict* controls over the information that can be collected, stored, and disseminated. No procedural or technical safeguard is immune from human abuse or mechanical failure.

Certain types of information should not be recorded even if it is technically feasible to do so and some administrative objective would be served thereby. It has long been technically "feasible" and, from some perspectives, "desirable" to require citizens to carry and display passports when moving through the country, or to require universal fingerprinting. But the United States has not pursued these objectives because they are considered inconsistent with the philosophical fibre of our society. By the same token, absent an overpowering demonstration that the preservation of sensitive or highly personal information, such as medical and psychiatric information, or dossier-type information on those pursuing lawful political and social activities, is essential to some fundamental policy, the scrivener's hand should be stayed and the data permitted to be lost to man's memory or simply retained on a decentralized and highly confidential basis.

Another form of self-regulation that seems essential is limiting access to data. The hardware and software of any system dealing with personalized information must be designated to limit the exposure of files to a limited class of people whose access is authorized only after a careful examination

of their need to know. Everyone making an inquiry into an individual file must be required to identify himself. But it must be remembered that an identification code number assigned to each user or a magnetically coded identification card can easily be lost, stolen, or exchanged. Thus, ultimately, finger or voice prints may prove to be necessary. In addition, the system should be equipped with protector files to record the identity of inquirers and these records should be audited periodically to determine whether the system is being misused by those who have a legitimate right of access. In the same vein, it probably will be necessary to audit the programs controlling the manipulation of the files to make sure that no one has inserted a secret "door" in the protective software or modified it so that a particular password will permit access to the data by unauthorized personnel.

Because it is possible to move information into or out of a computer over substantial distances by telephone lines or microwave relays connected to terminals scattered throughout the country and even beyond, it is essential that information be protected against wiretapping and other forms of electronic eavesdropping. This risk can be minimized by coding the data or using "scramblers" to garble the information before transmission and installing complementary devices in the authorized terminals to reconstitute the signal. These procedures also will prevent "piggy-backing" or "infiltrating" the system by surreptitiously attaching a terminal to an authorized user's transmission line.

To insure the accuracy of computerized files, an individual should have access to any information in his dossier and an opportunity to challenge its accuracy. This principle has been recognized and is embodied in a new federal statute—the Fair Credit Reporting Act.[7] This enactment is the first step toward eliminating some of the abuses that result from the buying and selling of personal information by consumer reporting companies, most notably credit bureaus. It gives us a right of access to the files maintained on us by these organizations, provides a procedure for correcting any errors we might find, assures us of notice when adverse decisions are made on the basis of a consumer report, and places some restraints on the investigative reporting conducted by these firms. Although the act is full of loopholes, its basic philosophical premise, that an individual has a right to see his file, is sound and must be extended to other contexts.

Another approach might be to send a person's record to him once a year. This suggestion obviously may prove expensive, some will argue that the value of certain information will be damaged if its existence and recordation are disclosed, and it *might* produce a flow of petty squabbles that would entail costly and debilitating administrative or judicial proceedings. Nevertheless, the right of an individual to be protected against the dissemination of misinformation about him is so important that some price must be paid to effectuate it.

Finally, the information must not be allowed to petrify. Data that is shown to be inaccurate, or archaic, or of little probative value, should be deleted, reclassified, or its age brought to the attention of a user of the file.

But what if self-regulation fails? Indeed, can we afford the luxury of waiting to find out? It seems clear to me that the legal profession must become more active in finding a solution to the computer-privacy dilemma. Unfortunately, we cannot be too sanguine about the existing legal structure's ability to meet the challenge. The common law of privacy traditionally has been preoccupied with the problems raised by the mass media and has concerned itself with the commercial exploitation of a name or likeness, the offensive intrusion into an individual's personal affairs, the widespread public disclosure of private information, and the "false light" cast on individuals by media disclosures.[8]

In the constitutional law arena, recent cases seeking the expungement of files maintained by law enforcement agencies have been largely unsuccessful.[9] Despite strong arguments that the preservation of detailed information directly infringes the data subjects' right of associational privacy under the first amendment, no relief usually is given because of a judicial concern over the government's need to be able to deal with lawlessness. Furthermore, any privacy action based on constitutional rights will have to avoid the inhibiting effect of the Supreme Court's decision in *Time, Inc. v. Hill,*[10] which imposes a heavy burden of proof on the party seeking relief for an invasion of privacy.[11] The effect of that case is to give the media substantial immunity from liability for invasions of privacy in order to provide "breathing space" for freedom of expression. I think it is fair to say that this decision partially aborts the common law right of privacy's capacity for doctrinal growth.

The judicial vineyards are not completely blighted, however. The right of associational privacy is probably the most clearly developed of the constitutional protections for personal information. Thus, when the government attempts to gather data from an individual concerning his association with a group dedicated to the advancement of certain beliefs, it must show that the information sought is a subject of overriding and compelling state interest.[12] Closely related to associational privacy is another type of privacy that the courts have protected—the right to possess ideas and beliefs free from governmental intrusion. The leading case in this area, *Schneider v. Smith,* [13] makes it clear that espousing an unpopular idea is not a scar a person must show upon inquiry for the remainder of his life.

In a related field, a number of cases protect our physical privacy from unreasonable searches and seizures and guarantee us the "right to be let alone" in what have been described as "zones of privacy." [14] This view is exemplified by *Griswold v. Connecticut,* [15] which struck down Connecticut's attempt to regulate the use of contraceptive devices. However, a recent Supreme Court decision upholding the right of welfare authorities to terminate benefits if they are not given access to the welfare beneficiary's home under certain circumstances seems to look the other way.[16] On the plus side, mention also should be made of *Wisconsin v. Constantineau,*[17] which appears to have infused due process notions into the use of information by requiring that when a person's reputation, honor, or integrity is jeopardized by a governmental dissemination of personal information, a minimal level of procedural fairness must be satisfied. But peculiarities in *Constantineau* caution us against expecting too much from it.

But these decisions simply represent the outer boundaries or constitutional limits on governmental action—they do not give us the standard for achieving the balance that is desperately needed. That will have to come from the legislature. Legislative activity in the computer-privacy field might take a number of different forms. One simple and highly desirable statutory approach would be to prohibit governmental, and perhaps even nongovernmental, organizations from collecting designated classes of sensitive data. This might be reinforced by a statutory requirement and computerized files be periodically purged of all data that has become too ancient to be trustworthy. Of course, any proposal that would have the effect of impeding the government's information practices faces an uphill battle in the political arena.

A somewhat different, and in many ways more drastic legislative approach, involves requiring computer manufacturers, users, and data networks to employ prescribed safeguards for maintaining the integrity of personal information. This can take

[7] Pub. L. No. 91-508, 84 Stat. 1127-36, 15 U.S.C. §§ 1601-77 (1970).

[8] *See* A. Miller, *supra* note 5, at 173-89.

[9] *See* Anderson v. Sills, 56 N.J. 210, 265 A.2d 678 (1970), *rev'g* 106 N.J. Super. 545, 256 A.2d 298 (1969). *See also* Menard v. Mitchell, 430 F.2d 486 (D.C. Cir. 1970). Judge Gesell's opinion on remand in the *Menard* case reflects a very balanced and sophisticated approach to the data bank question. Menard v. Mitchell, Civil No. 39-68 (D. D.C. June 15, 1971).

[10] 385 U.S. 374, 87 S. Ct. 534 (1967).

[11] *See* A. Miller, *supra* note 5, at 190-99.

[12] *See* NAACP v. Alabama, 357 U.S. 449, 78 S. Ct. 1163 (1958). *See also* Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539, 83 S. Ct. 889 (1963).

[13] 390 U.S. 17, 88 S. Ct. 682 (1968).

[14] *See* Stanley v. Georgia, 394 U.S. 557, 89 S. Ct. 1243 (1969); Katz v. United States, 389 U.S. 347, 350 n.5, 88 S. Ct. 507, 510-11 n.5 (1967); Berger v. New York, 388 U.S. 41, 87 S. Ct. 1873 (1967).

[15] 381 U.S. 479, 85 S. Ct. 1678 (1965).

[16] Wyman v. James, 400 U.S. 309, 91 S. Ct. 381 (1971). *See generally* Burt, *Forcing Protection on Children and Their Parents: The Impact of Wyman v. James,* 69 *Mich. L. Rev.* 1259 (1971). *See also* Law Students Civil Rights Research Council, Inc. v. Wadmond, 401 U.S. 154, 91 S. Ct. 744 (1971).

[17] 400 U.S. 433, 91 S. Ct. 507 (1971).

the form of (1) imposing a statutory duty of care on everyone connected with the data-handling process, which would encourage privacy consciousness, or of (2) enacting detailed privacy-oriented technical requirements, which would have to be followed by computer manufacturers. These would include sophisticated protective schemes involving access regulations, personnel controls, and mechanical devices that can discriminate among users and differentiate data on the basis of sensitivity that would have to be complied with by handlers of personal information.

But detailed congressional legislation is difficult to draft and the best solution may be to give over the task of regulation to an administrative agency that would act as an information ombudsman or a privacy auditor. The notion of an independent information agency is not a new one. Many of the congressional witnesses and commentators on the proposal to create a National Data Center, myself included, stressed the importance of locating control of such an organization outside the existing regulatory framework.[18] Administrative regulation would obviate the need to make highly detailed policy judgments in statutory form at what may be a premature time. It also would guarantee that the problem is placed in the hands of a watchdog group, hopefully composed of experts drawn from many fields, that could exercise continuing supervision over the data handling community.[19]

A number of Congressmen already have recognized the need for some controls and have introduced legislation to protect privacy. Unfortunately, the activity is somewhat reminiscent of Leacock's Man, who jumped on his horse and rode off in all directions at once. Bills have appeared to regulate credit bureaus, mailing list companies, the census, employee privacy, government inquiries, and psychological testing. Thus far only the Fair Credit Reporting Act, mentioned earlier has been enacted into law. But Senator Ervin and Congressmen Gallagher and Koch have proposed broad regulation of computers and data gathering activities and we can expect continued activity in this field for some time.

When the dust ultimately settles, I hope we shall have struck the necessary balance. This probably will require give on both sides. No doubt we can coerce, wheedle, and cajole an individual into giving up part, or even all, of his informational profile. But what price would we pay for it? Alienation, distrust of the government, deceptive responses, obfuscation of certain data gathering objectives (as I think may be true of the census goal of enumerating the population), numbing of privacy values, and an atmosphere of suspicion. Instead of the stick, perhaps we should rely on the carrot. Governmental and private planners must refine their information handling techniques, reduce the burden on the individual, and assure us accuracy of the files and security against improper dissemination. If this is done, perhaps we will feel less apprehensive about yielding a little of ourselves. Few aspects of life, even in a free society, can survive as absolutes—and that includes privacy.

If some of my remarks seem slightly alarmist in tone, it is because I feel it is necessary to counteract the syndrome referred to by the poet e.e. cummings, when he wrote "progress is a comfortable disease." [20] We must overcome the all-too-often complacent attitude of citizens toward the management of our affairs by what frequently are astigmatic administrators in both government and the private sector. The very real benefits conferred by information technology may opiate our awareness of the price that may be exacted in terms of personal freedom. It thus seems desirable to sound the klaxon to arouse a greater awareness of the possibility that the computer is precipitating a realignment in the patterns of societal power and is becoming an increasingly important decision-making tool in practically all of our significant governmental and nongovernmental institutions. As society becomes more and more information oriented, the central issue that emerges to challenge us is how to contain the excesses and channel the benefits of this new form of power.

If the concept of personal privacy is fundamental to our tradition of individual autonomy, and if its preservation is deemed desirable, then I feel that the expenditure of some verbal horsepower on its behalf is justified. Unless we overcome inertia, there will be no one to blame but ourselves if some day we discover that the mantle of policymaking is being worn by those specially trained technicians who have found the time to master the machine and are using it for their own purposes. To paraphrase the French sociologist, Jacques Ellul, that it is to be a dictatorship of dossiers and data banks rather than of hobnailed boots will not make it any less a dictatorship.[21]

[18] *See Hearings on Computer Privacy Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary*, 90th Cong., 2d Sess. (1968) (statement of Professor Arthur R. Miller); Note, *Privacy and Efficient Government: Proposals for a National Data Center*, 82 *Harv. L. Rev.* 400, 404 (1968). *See also* Ruggles, *On the Needs and Values of Data Banks*, in *Symposium—Computers, Data Banks, and Individual Privacy*, 53 *Minn. L. Rev.* 211, 218–19 (1963); Zwick, *A National Data Center*, in A.B.A. Section of Individual Rights and Responsibilities, Monograph No. 1, at 32, 33 (1967).

[19] This theme is developed in A. Miller, *supra* note 5, at 228–38.

[20] e.e. cummings, *100 Selected Poems* 89 (paperback ed. 1959).

[21] J. Ellul, *The Technological Society* 434 (paperback ed. 1964).

RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS *

by Willis H. Ware

IN EARLY 1972, then Secretary of Health, Education and Welfare Elliot Richardson, created a special advisory committee charged with analyzing harmful consequences that might result from automated personal data systems, and which was to make recommendations about safeguards that might protect individuals against potentially harmful consequences and afford them redress for any harm. Since the social security number has been widely used as a personal identifier, the committee was also asked to examine the policy and practice relating to the issuance and use of such numbers. On July 31, 1973, the committee submitted its final report to current H.E.W. Secretary Casper Weinberger, with Attorney General Elliot Richardson in attendance. **

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

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

It is helpful to review suggestions that have been made to deal with the matter of protecting data subjects against harm. One proposal has been to license and certify computer programmers and systems designers, with the hope that such a procedure would improve the care with which record-keeping systems are designed and operated. While assuredly useful, it cannot of itself adequately protect data subjects against potential harm. The best designed system in the world cannot prevent authorized users of the system from maliciously using the information. More to the point, however, a certification approach would put the responsibility for a properly designed and controlled record system in the wrong place. The responsibility should be upon the organization that assembles the system, initiates its design and operates it, not upon the technical professionals who implement it.

A second suggestion is the ombudsman approach that has been used for many years in Scandinavian countries. Basically, the ombudsman is a spokesman for an individual who has been harmed; he serves essentially as a communication channel between the person and a bureaucracy in matters of dispute. While the concept is a useful third-party mechanism to facilitate resolution of an argument, it is not well-established in this country, nor is it a sufficiently broad and powerful force to bring about essential changes in how record-keeping systems are designed and deterred from inappropriate behavior.

There have been many definitions of privacy, all of which contain the common element that personal data is bound to be disclosed and that the data subject should have some hand in deciding the nature and extent of such disclosure. As the committee phrased it, "personal privacy as it relates to personal-data record keeping must be understood in terms of a concept of mutuality." The organization that holds personal data must not have complete control over it and, conversely, neither may the data subject—each has a stake in seeing that the information is used properly. As part of the committee's definition of privacy, it was suggested that, "a record containing information about an individual in identifiable form must . . . be governed by procedures that afford the individual a right to participate in deciding what the content of the record will be and what disclosure and use will be made of the identifiable information in it. Any recording, disclosure and use of identifiable personal information not governed by such procedures must be proscribed as an unfair information practice unless such recording, disclosure or use is specifically authorized by law."

Thus, the committee concluded that safeguards for personal privacy based on such a concept of mutuality in record-keeping, requires adherence by record-keeping organizations to certain fundamental principles which collectively define *fair information practice*. We proposed that:

> There must be no personal-data record-keeping systems whose very existence is secret.
>
> There must be a way for an individual to find out what information about him is in the record and how it is used.
>
> There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
>
> There must be a way for an individual to correct or amend a record of identifiable information about him.
>
> 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.

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

Thus, the committee has proposed a solution that was felt to provide the citizen with equally strong rights, while at the same time avoiding the necessity for a regulatory body. It has recommended that there be created by legislation a code of fair information practice applicable to all automated personal data systems. This code would define "fair information practice" as adherence to specified safeguard requirements, would prohibit violation of any requirement as an unfair information practice, would provide both civil and criminal penalties for unfair information practice, would provide for injunctions to prevent violation of any safeguard requirements and, finally, would permit both individual and class action suits for actual liquidated and

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

punitive damages. This approach, the committee is convinced, would not impose constraints on the application of EDP technology beyond those necessary to assure the maintenance of reasonable standards of personal privacy in record-keeping. It would imply no new federal bureaucracy, and enforcement should be inexpensive at the government level. Importantly, this approach exploits the established legal and judicial institutions and practices of the country, and through court decisions and judgments can provide an adaptable solution that reflects shifts in the attitudes of society. From the standpoint of industry, the monitoring of fair information practice would become a matter for the General Counsel's office, as he is already concerned with fair labor practice and other requirements levied by law.

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

To implement such a fair information practices code we suggest certain safeguard requirements. One set stipulates that:

> any organization maintaining an administrative automated personal data system shall identify one person immediately responsible for the system, shall take affirmative action to inform each of its employees about the safeguard requirements and rules and procedures governing the conduct of the system,
>
> shall specify penalties to be applied to any employees who violate the safeguard,
>
> shall take reasonable precautions to protect data in the system from anticipated threats or hazards to the security of the system,
>
> shall make no transfer of identifiable personal data to another system unless such other system also fulfills the safeguard requirements, etc.

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

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

> Shall inform an individual when asked to supply personal data whether he is legally required or may refuse to supply the data requested.
>
> Shall inform an individual upon request whether he is the subject of data in the system and, if so, make such data fully available to him.
>
> Shall assure that no use of individually identifiable data is made that is not within the stated purposes of the system.
>
> Shall inform an individual, upon request, about the uses made of data about him, including the identity of all persons and organizations involved and their relations with the system.
>
> Shall assure that no data about an individual are made available in response to a demand for data by means of compulsory legal process unless the individual to whom the data pertains has been notified of the demand.
>
> Shall maintain procedures that allow an individual who is the subject of data in the system to contest their accuracy, completeness, pertinence, and the necessity for retaining them; that permit data to be corrected or amended when the individual so requests, and assure when there is disagreement that the individual's claim is noted and included in any subsequent disclosure or dissemination of the disputed data.

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

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

The second major issue to be considered by the committee was that of the social security number and its growing status as a standard universal identifier. The initial press coverage of our report stated simply that we were against the use of the social security number as a personal identifier but excluded the supporting arguments.

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

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

Meanwhile, in order to constrain the spread of the SSN as a *de facto* standard identifier, we recommend that

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

To further restrict the spread of the SSN in its identifier role, we recommend that legislation be passed that:

> Gives the individual a legal right to refuse to disclose his social security number to any person or organization that does not have specific federal authority to request it.
>
> Provides that an individual have the right to redress if his lawful refusal to disclose his social security number results in the denial of a benefit or the threat of denial of a benefit.
>
> Requires that any oral or written request made to an individual for his social security number be accompanied by a clear statement indicating whether or not compliance with the request is required by federal statute and, if so, citing the specific legal requirement.

We have also made a number of other recommendations with regard to the SSN, the net effect of which is to restrict its use to those purposes mandated by federal law, to urge the Social Security

APPENDIX VII

Administration not to assign numbers to children below ninth grade level, and to give the SSN the status of a confidential item of information.

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

Appendix VIII

DATABANKS IN A FREE SOCIETY: A SUMMARY OF THE PROJECT ON COMPUTER DATABANKS *

by Professor Alan F. Westin
Department of Political Science, Columbia University

Based on a summary of the Project on Computer Databanks and of its report "Databanks in a Free Society" published 1972 by Quadrangle Books, a New York Times Company, 330 Madison Ave., New York, N.Y. 10017.

THE UNITED STATES HAS BECOME A RECORDS-ORIENTED SOCIETY.

In each major zone of personal and civic life (education, employment, credit, taxation, health, welfare, licensing, law enforcement, etc.), formal, cumulative records are assembled about each of us by hundreds of private and government record-keeping organizations. These personal histories are relied on heavily by the collecting organizations in making many decisions about our rights, benefits, and opportunities. Informal networks for sharing record-information among public and private organizations have become a common feature of organizational life heavily dependent on credentials.

During the past two decades, as most government agencies and private organizations have been computerizing their large-scale files, the American public has become concerned that dangerous changes might be taking place in this record-keeping process. Because of the computer's enormous capacities to record, store, process, and distribute data, at great speeds and in enormous volumes, many people have feared that far more personal data might be assembled about the individual than it had been feasible to collect before; that much greater sharing of confidential information might take place among the holders of computerized records; and that there might be a lessening of the individual's ability to know what records have been created about him, and to challenge their accuracy or completeness.

The book *Databanks in a Free Society* (currently being published by Quadrangle Books, a *New York Times* subsidiary) is the report of the first nationwide, factual study of what the use of computers is *actually* doing to record-keeping processes in the United States, and what the growth of large-scale databanks, both manual and computerized, implies for the citizen's constitutional rights to privacy and due process. This article is a summary of the book. The book also outlines the kinds of public policy issues about the use of databanks in the 1970's that must be resolved if a proper balance between the individual's civil liberties and society's needs for information, is to be achieved.

How the Study was Conducted

The book is the report of the "Project on Computer Data Banks", a three-year research study conducted under the auspices of the Computer Science and Engineering Board of the National Academy of Sciences, under grants of $164,000 from the Russell Sage Foundation. The Director of the Project was Dr. Alan F. Westin, Professor of Public Law and Government, Columbia University, and author of *Privacy and Freedom,* published in 1967. An inter-disciplinary staff of seven scholars from the fields of law, computer science, and the social sciences collaborated in the research. The project received continuing guidance not only from the Computer Science and Engineering Board but also a special Advisory Board of 18 prominent figures in public life whose views spanned the full spectrum of opinion on issues of databanks and civil liberties.* The final report of the project was written by Dr. Westin and Mr. Michael A. Baker, Assistant Director of the Project and an Instructor in Sociology at Brooklyn College of the City University of New York.

Sources

The major sources collected and used by the Project include:

1. Documentary materials on computerized record systems in more than 500 government agencies and private organizations.
2. Detailed on-site staff visits to 55 of the most advanced computerizing organizations, ranging across the most sensitive fields of personal record-keeping.

* Reprinted with permission from *"Computers and Automation,"* January 1973, copyright 1973 by and published by Berkeley Enterprises, Inc., 815 Washington St., Newtonville, Mass. 02160.

* Names of staff and Advisory Board members appear later in this summary.

3. Replies from over 1500 organizations in a national mail survey of developments in computerization and record-keeping among government agencies and private organizations.
4. Extensive interviews with officials from computer companies, software houses, systems consulting firms, industry associations, civil liberties groups, labor unions, consumer organizations, minority-rights organizations, and professional associations.
5. Legal, legislative and regulatory-agency materials dealing with databank issues in 25 distinct major fields of personal record-keeping.
6. Materials and interviews on the state of databank developments and regulatory controls in 23 foreign nations, for purposes of comparison with the United States.

Organization of the Report

The Report is organized into five parts:

Part I presents a brief, orienting discussion of computer systems and civil liberties concepts for general readers.

Part II consists of "profiles" of 14 governmental, commercial, and private organizations, drawn from the 55 to which the Project staff made on-site visits. Each profile describes the nature and function of the organization, its pre-computer record-keeping, its move into computer usage, the effect of automation on its record-keeping about people, previous civil liberties issues involving the organization's manual record-keeping, the effect of computerization on civil liberties protections, and the organization's plans for further computerization in the next five years.

The 14 organizations given this detail treatment are:

The U.S. Social Security Administration
The F.B.I.'s National Crime Information Center
Kansas City (Missouri) Police Department
New York State Department of Motor Vehicles
City of New Haven, Connecticut
Santa Clara County, California
Bank of America
TRW—Credit Data Corporation
Mutual of Omaha Insurance Company
R. L. Polk & Company
Massachusetts Intsitute of Technology
Church of Latter Day Saints
Office of Research, American Council on Education
Kaiser-Permanente Health Plan

Part III has three chapters which present and analyze the Project's principal findings. These include an overview of what kinds of files have and have not been computerized in advanced organizations; an analysis of computer effects on civil liberties that are *not* taking place as yet; and a description of those changes in record-keeping that the use of computers and communication systems *is* producing in these organizations.

Part IV is an analysis of the way in which the reception of computer technology is affected by organizational, legal, and socio-political factors, followed by a forecast of developments in new computer and communications technologies that are likely to occur in the remainder of the 1970's, and an analysis of their implications for civil liberties interests.

Part V discusses public policy choices in the 1970's in light of the project's findings and forecasts. The first chapter analyzes the larger socio-political significance of the computer's arrival in the late 1950's and 1960's; it goes on to suggest the basic civil liberties principles that ought to be followed when seeking to safeguard citizen rights in large-scale record systems, especially in the increasingly computerized sectors of American organizational life. The final chapter of the report presents an agenda for the 1970's, identifying six areas of priority for public policy and civic action.

Three appendixes to the report present: the results from the Project's survey of organizations; an analysis of public opinion literature on privacy and the computer; and information about the experience of other advanced industrial nations in dealing with the databanks-and-privacy problem.

Highlights of the Report

A great many commentators have warned that the spread of computers is fundamentally altering the balance between information policies of organizations and individual rights to privacy that marked past eras of record-keeping. Compared to what was done in the manual era, it is said, the new capacities of the computer *inevitably* lead organizations: to collect more detailed and intrusive personal information about individuals; to consolidate confidential information from previously separate files; and to share confidential personal data with government agencies and private organizations that had not received it before.

The Project's findings from visits to 55 organizations with highly advanced computer applications is that computerization is *not* yet having such effects in the overwhelming majority of such organizations. For a combination of technological and organizational reasons, central databank developments are far from being as advanced as many public commentaries have assumed. Organizations have so far failed to achieve the "total" consolidation of their information about individuals which raised civil liberties alarms when such goals were announced in the 1960's by various government agencies or private organizations.

Continuance of Policies

Further, in computerizing their records on individuals, organizations have generally carried over the same policies on data collection and sharing that law and administrative traditions in each field had set in the pre-computer era. Where new law or practices have evolved to protect individual liberties over the past decade, organizations with computerized systems have followed such new policies as fully as those that still use manual files and procedures. Even the most highly computerized organizations continue to rely heavily on manual record-keeping and retain in their paper files the most sensitive personal information they possess.

Another widely held fear is that computerization makes it more difficult for the individual to know what is in the file about him, to have errors corrected, or have the data erased where public policy specifies that certain information about an individual's past should be ignored.

The Project's inspection of advanced systems showed that notice to the individual about a record's existence, opportunity to inspect and challenge that record, and policies as to the removal of out-of-date or irrelevant information were not being substantially altered by computerization. Where policies affording individuals rights of due process such as the above had been provided in an organization prior to computerization, those rules are being followed in the new computerized systems as well. Where no such rights were given, the adoption of computers has not made the situation either worse or better. Neither has computerization introduced impersonal decision-making in systems where this was not present before, nor forced organizations into greater reliance on "the record" in making decisions about clients, customers or citizens. Where abuses along these lines were present in computerized systems—raising serious due process questions—they had been carried over from the high-volume "processing" of people in the manual era.

Public Misunderstanding

Over and over again, the Project's findings indicate profound public misunderstanding about the effect of computers on large scale record systems. To some extent, the inflated claims and proposals of organizational managers about the capacities of their computer systems helped to generate what were in fact baseless concerns for privacy on the part of the public.

In addition, as the Report shows with respect to law enforcement uses and airline-reservations and charge-card systems, many commentators on computers and privacy issues have failed to do adequate research into the actual operations of systems about which they write, and have presented entirely incorrect pictures to the press and public about how these computer systems work. The danger in this, the report points out, is that we may give up the fight in the belief we have already lost:

If we assume that computer users are already doing things that they are not, we risk surrendering without a fight the border between properly limited and surveillance-oriented computer applications. . . . The question of what border control measures should be adopted can hardly be understood and properly considered . . . if the public and opinion leaders assume that the borders have already been obliterated.

Efficiency

Computerization in advanced organizations *is* producing changes in record-keeping methods that can increase the efficiency with which organizations carry out their basic decision-making about the people they process or serve. Computerization is making it possible for many organizations to: maintain more up-to-date and complete records; obtain faster responses to inquiries about a given individual; and make more extensive use of information already in the files. Computers have also made possible dramatic expansion of networks for exchange of data among organizations that have shared data since pre-computer days; and the creation of some large data bases of information about people that would not have been feasible without automation. These changes have been felt already in police information systems, national credit reporting systems, charge card systems, and others.

Data-Sharing

Looking at technological trends for the remaining years of the 1970's, the Report forecasts that while there will be important continued increases in computer capabilities, no developments are now foreseeable that will alter the technological, organizational, and socio-political considerations that presently frame the databanks and civil liberties issue. Organizations will have more flexible, reliable, and cost-effective computer systems to use in pursuit of their policies, but these will not represent a radical departure from the computer capabilities presently available. The most important development with implications for civil liberties interests will be an increase in the ease with which data can be shared among organizations which have computers, coupled with a reduction in the cost of doing so. This will make it imperative that legal boundaries as to data-sharing are set as clearly as possible.

Augmenting the Power of Organizations

The Project concluded that the real issue of databanks and civil liberty facing the nation today is not that revolutionary new capacities for data surveillance have come into being as a result of computerization. The real issue is that computers arrived to augment the power of organizations just when the United States entered a period of fundamental debate over social policies and organizational practices, and when the traditional authority of government institutions and private organizations has become the object of wide-spread dissent.

Challenge of Goals

Important segments of the population have challenged the goals of major organizations that use personal records to control the rights, benefits, and opportunities of Americans. There is also debate over the criteria that are used to make such judgments (religious, racial, political, cultural, sexual, educational, etc.), and over the procedures by which the decisions are reached, especially those that involve secret proceedings and prevent individuals from having access to their own records.

Distrust of Organizational Record-Keeping

Computers are making the record-keeping of many organizations more efficient precisely at the moment when trust in many large organizations is low and when major segements of the American population are calling for changes in values that underly various social programs, for new definitions of personal rights, and for organizational authorities to make their decision-making procedures more open to public scrutiny and to the review of specific individuals involved.

Little Legislation

Despite the rapid spread of computers, there has been little so far by way of new legislation, judicial rulings, regulatory agency rules, or other legal remedies defining new rights to privacy and due process in major record systems. The Report stresses that, because of the increased efficiency of record-keeping and the growing intensity of the public's concern, the middle 1970's is the moment when law-makers and the public must confront both long-standing and newly-raised civil liberties issues, and evolve a new structure of law and policy to apply principles of privacy and due process to large-scale record-keeping.

The Report identifies six areas of priority for public action, and presents examples of specific policy measures under each of these that ought to be seriously considered by policy makers.

Right of Access and Challenge

Development of laws to give the individual a right of access and challenge to almost every file in which records about him are kept by city, county, state, or government agencies: At stake here is the possibility that, denied access to records being used for decisions about himself, the citizen is left with "feelings of powerlessness and the conviction that government authority is fundamentally arbitrary."

At the very least, citizens ought to know what record systems exist in government agencies. A Citizen's Guide to Files, published at every appropriate level of government jurisdiction, should "provide the citizen with a thorough, detailed and non-technical directory of the record systems that contain information about him, and the general rules under which it is being held and used." Providing adequated due process protection in government files, the Report suggests, is best achieved by assuming that any individual should be able to see and get a copy of any records used to affect him or her personally—with the record-keeping agency "bearing the burden of proving that some specific public interest justifies denying access."

Explicit Rules

Develop of explicit laws or rules balancing confidentiality and data-sharing in many sensitive record systems that today do not have clearly defined rules: Among these would be rules governing the provision of information to law enforcement agencies from bank accounts, travel and entertainment card records, airline and hotel reservation systems, etc. The Report predicts that one or two large systems will come to dominate in each of these areas.

> This development will make the individual's account record more comprehensive and a very inviting target for investigators of all kinds. With that rise in sensitivity and attractivenes ought to go legislative enactments spelling out retention and destruction policies confidentiality rules, and procedures for protecting individual rights when outsiders seek to obtain access for what are asserted to be lawful and necessary purposes.

As a case study in how not to build new record systems, the Report discusses some of the major Administration and Congressional proposals for national welfare reform, which generally hinge on the availability of computers for massive data storage and exchange. Several of the welfare system proposals contain "sweeping authorizations for data collection and sharing but almost nothing by way of confidentiality standards and due-process review procedures." The Report points out that we may be "creating one of the largest, most sensitive, and highly computerized record systems in the nation's history, without explicit protections for the civil liberties of millions of persons whose lives will be profoundly affected . . ."

Records of the Wrong Kind

Limit the collection of personal information where a proper regard for the citizen's right to privacy suggests that records ought not to be maintained at all by certain organizations, or never furnished for certain uses in the society: Among the examples are the use of arrest-only records in licensing and employment decisions, and the selling to commercial advertising services of names and addresses collected by government under its licens-

ing and regulatory powers, unless the individual specifically consents to such use.

In the case of arrest records, the Report stresses that:

> A democratic society should not allow arrest records to be collected and circulated nationwide with increasing efficiency without considering directly the actual social impact of their use in the employment and licensing spheres, and without examining the possibility that dissemination beyond law-enforcement agencies represents an official stigmatization of the citizen that ought to be either forbidden by law, or closely regulated.

Social Policy

Increased work by the computer industry and professionals within it on technological safeguards which will make it possible to implement confidentiality policies more effectively than is now feasible: The Report notes that:

> No 'technological fix' can be applied to the data-bank problem. Protection of privacy is a matter of social policy, on which computer professionals are fellow-citizens, not experts.

But the Project calls for more research, development and testing efforts to be undertaken by the computer industry to see that the computer's capacities for protection of confidentiality and insurance of proper citizen access are turned into "available and workable products". Law and public pressure, the Report suggests, require that such measures be taken by managers of sensitive record systems when they are computerized, thereby stimulating the "user demand" to provide a practical market for such devices and techniques.

No Extension of Use of Social Security Number

Reconsideration by Congress and the executive branch of the current permissive policies toward use of the social security number in an increasing number of government and private record systems: The Report notes that having such a number is not a prerequisite for linking files within or between organizations, but notes that a common numbering system clearly makes record linkage easier and cheaper. Further, the Project concludes that resolving the critical civil liberties issues in record keeping "will require that a minimum level of trust be maintained between American citizens and their government. Under these conditions, adopting the social security number as a national identifier or letting its use spread unchecked cannot help but contribute to public distrust of government."

Information-Trust Agencies

Experimentation with special information-trust agencies to hold particularly sensitive bodies of personal data: For example, the Report suggests that the handling of both national crime statistics and summary criminal histories ("rap sheets") might be taken away from the Federal Bureau of Investigation and placed in an independent national agency under control of a board that would have public representatives as well as law enforcement officials on it. Such an agency would have to be established "with a clear legislative mandate to be a 'guardian' institution," paying attention to civil liberties interests as well as law enforcement needs.

Critical Period, 1973-78

The Report stressed that the next five years would be a critical period in the reception and control of sensitive personal record systems, especially those managed by computers. More sensitive areas of record-keeping are being entered by many computerizing organizations; many larger on-line (instant access) networks are being brought into operation; and more consolidations of presently scattered records about individuals can be seen as a trend in certain areas, such as criminal justice, credit and financial transactions, and welfare. The Report stresses that unless lawmakers and organizational managers develop proper safeguards for privacy and due process, and create mechanisms for public scrutiny and review, the record systems they are building could sharpen the already serious debate in American society over the way to apportion rights, benefits, and opportunities in a credential-oriented society, and leave organizational uses of records to control individual features too far outside the rule of law.

In its closing paragraphs, the Report sums up the databanks and civil liberties problem as follows:

> If our empirical findings showed anything, they indicate that man is still in charge of the machines. What is collected, for what purposes, with whom information is shared, and what opportunities individuals have to see and contest records are all matters of policy choice, not technological determinism. Man cannot escape his social or moral responsibilities by murmuring feebly that "the Machine made me do it." There is also a powerful tendency to romanticize the pre-computer era as a time of robust privacy, respect for individuality in organizations, and "face-to-face" relations in decision-making. Such arcadian notions delude us. In every age, limiting the arbitrary use of power, applying broad principles of civil liberty to the troubles and challenges of that time, and using technology to advance the social well-being of the nation represent terribly hard questions of public policy, and always will. We do not help resolve our current dilemmas by thinking that earlier ages had magic answers.
>
> Computers are here to stay. So are large organizations and the need for data. So is the American commitment to civil liberty. Equally real are the social cleavages and cultural reassessments that mark our era. Our task is to see that appropriate safeguards for the individual's rights to privacy, confidentiality, and due process are embedded in every major record system in the nation, particularly the computerizing systems that promise to be the setting for most important organizational uses of information affecting individuals in the coming decades.

Staff Associates for the Project

Robert F. Boruch, Assistant Professor, Department of Psychology, Northwestern University

Howard Campaigne, Professor of Mathematics, Slippery Rock State College

Gerald L. Grotta, Associate Professor of Journalism, Southern Illinois University

Lance J. Hoffman, Assistant Professor of Electrical Engineering and Computer Sciences, University of California, Berkeley

Charles Lister, Attorney at Law, Washington, D.C.

Advisory Group

The Project had during its existence an Advisory Group that provided the staff with a wide range of diverse viewpoints on the databanks and civil liberties issue and helped shape the project's studies. Members of the Advisory Group were:

Edgar S. Dunn, Jr.
Resources for the Future, Inc.

The Honorable Cornelius E. Gallagher
House of Representatives

Richard Freund
First National City Bank

Justice Nathan L. Jacobs
New Jersey Supreme Court

Nicholas deB. Katzenbach
Vice President and General Counsel, IBM Corp.

John H. Knowles
President, Rockefeller Foundation

Arthur R. Miller
Professor of Law, Harvard University Law School

George A. Miller
Institute for Advanced Study, Princeton, N.J.

Ralph Nader
Attorney, Washington, D.C.

Arthur Naftalin
Professor of Public Affairs, Univ. of Minnesota

Anthony G. Oettinger
Harvard University

John R. Pierce
California Institute of Technology

The Honorable Ogden R. Reid
House of Representatives

APPENDIX VIII

L.F. Reiser
Corporate Director, Personnel and Industrial Relations, CPC International Inc.

Richard Ruggles
Department of Economics, Yale University

Roderick O. Symmes
Director, Data Systems & Statistics Staff, U.S. Depart. of Housing and Urban Development

Roy Nutt
Vice President, Computer Sciences Corporation

Appendix IX

JUVENILE INFORMATION SYSTEMS: A COMPARATIVE ANALYSIS *

by Michael L. Altman

IN 1967, the President's Commission on Law Enforcement and Administration of Justice recommended that the Department of Justice and the States establish computer-based information systems for the purpose of "having complete and timely information about crimes and offenders available at the right place and the right time . . ." [1] Influenced by this recommendation, lured by the millions of dollars provided by LEAA,[2] and assisted by a Model Act, Model Regulations and Technical Memoranda prepared by Project SEARCH,[3] a large number of states and local jurisdictions have established automated criminal history systems.[4] Information pertaining to juvenile record systems is limited, but a 1972 Department of Justice survey [5] indicates that at least twenty-seven jurisdictions have introduced some form of automation into their juvenile courts. In addition, it is clear that many other juvenile courts are seriously contemplating adopting some form of automation into their record keeping practices.

The automation of juvenile records has clearly lagged behind the automation of adult criminal records. The reasons for this lag are not entirely clear for the juvenile justice system, which is compelled to serve both welfare and punitive goals, collects, stores and purports to utilize far more information than the criminal justice system. The need to manage this vast quantity of information would seem to have compelled the juvenile justice system to lead the movement towards automation—but, it hasn't. Based upon conversations with officials in several states, this seeming anomaly is explained in several ways: 1) Project SEARCH specifically excluded juvenile records from its model act,[6] 2) the fear that public opposition to automating juvenile records would jeopardize the movement toward automation of adult criminal records, 3) the belief that automating juvenile records might make it more difficult to preserve the historic principle that juvenile records should be confidential, 4) the belief computers don't forget and that a juvenile justice system exists, at least in part, so that we can both forgive and forget, 5) the belief of law enforcement presonnel that juveniles are different and that there is not as great a need for record information pertaining to juveniles as there is for adults and 6) the belief that the important information pertaining to juvenile is not a summary of previous offenses but rather background, social, and psychological data which is much more difficult and costly to quantify and store in an automated system.

These explanations are not entirely satisfactory because it is often asserted that computers can be programmed to preserve confidentiality (through the use of access codes, creating a log of those who seek information, etc.) and can be programmed to forget.[7] In addition, the national practice of diversion on the police level[8] would seem to indicate that law enforcement personnel would need and want accurate information quickly in order to make a diversion decision as [illegible] as possible. Also, a substantial percentage (22.6 percent) of all police arrests for violent crime are persons who are under the age of 18[9] and the reasons that law enforcement supports automated criminal histories pertaining to adults

* Reprinted from *Computer Applications in the Juvenile Justice System*, published by the National Council of Juvenile Court Judges.

[1] *The Challenge of Crime in a Free Society*, A Report by the President's Commission on Law Enforcement and Administration of Justic (1967) at p. 266.

[2] *Law Enforcement Assistance Administration* created by Title I of the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3701 (as amended by Public Law 93-83, August 6, 1973).

[3] SEARCH is an acronym for *System for Electronic Analysis and Retrieval of Criminal Histories*. The Project is located in Sacramento, California, is funded by LEAA and has produced a number of memoranda pertaining to automated criminal history systems including a Model Act (Technical Memorandum No. 3, May, 1971) and Model Regulations (Technical Memorandum No. 4, March, 1972).

[4] *The 1972 Directory of Automated Criminal Justice Information Systems*, published by the United States Department of Justice, reports that a survey of the 50 states and 103 local jurisdictions revealed 454 separate automated systems.

[5] *Id.* at D-33, 34.

[6] *Project SEARCH*, Technical Memorandum No. 4, Reg. 4 at pp. 3, 49 (March, 1972).

[7] The notion that the use of computers can limit rather than enhance risks to privacy is touted by computer salesmen and is accepted by *Project SEARCH*. *See*, Security and Privacy Considerations in Criminal History Systems, Project SEARCH Technical Report No. 2 (July, 1970). The notion is disputed by Professor Miller. Miller, A.R., *The Assault on Privacy* 41-53 (1971).

[8] Forty-nine and two-tenths percent of all juveniles taken into custody by the police in 1972 were not referred to juvenile court but were handled internally by the department or were referred to another agency. Crime in the United States: Uniform Crime Reports, Table 21, p. 116 (1972).

[9] Crime in the United States: Uniform Crime Reports, Table 21, p. 116 (1972).

would seem to apply at least to that class of juveniles. Finally, all of the explanations offered relate to the automation of records pertaining to identifiable juveniles and do not relate to the juvenile justice system's need for quantitative data collected for administrative and evaluative purposes.

Even if the explanations given for the reluctance to automate juvenile records are not totally adequate, there are a number of reasons that the emerging movement towards automation should proceed cautiously. First, although there may seem to be an internal logic dictating that we automate that information pertaining to juveniles which has been automated in the adult system, the fact is that many of the basic premises of the adult criminal history system, as well as its operation, are questionable. For example, the supposed prototype automated criminal history system, the NCIC system, has produced substantial criticism[10] ranging across the political spectrum from the American Civil Liberties Union to Senator Barry Goldwater. Most recently, the Governor of Massachusetts announced that Massachusetts would not participate in the NCIC system, "until such time as the Department of Justice or the Congress provides sufficient guarantees to safeguard individual rights and the system's integrity against abuse."[11] Since one of the basic principles of the juvenile justice system has been to preserve the confidentiality of a juvenile's contacts with the system in order to enhance the possibility of rehabilitation and decrease the possibility of stigma, the juvenile justice system should certainly pause until it is somewhat clearer whether automation will serve or disserve the interests of privacy and confidentiality. Stated another way, a major premise of the juvenile justice system is that children are different and that one of the ways that the system should recognize that difference is by giving children "another chance." One way in which a child is given another chance is by protecting his record so that he won't be treated as a "criminal." The importance of that value may require that we not automate juvenile records (notwithstanding some benefits produced by automation) because the risks would simply be too great that a basic premise of the system could be undermined.[12]

A second reason that juvenile courts should proceed cautiously with respect to a decision to automate its record systems is that the juvenile justice system, notwithstanding *Gault,* is premised upon a social-welfare model. That is, the system, as expressed through its diversion, intake and disposition mechanisms, is primarily concerned with what the child is (or isn't) and what he needs and not with what he did.[13] In order to find out what the child is and what he needs a detailed social history is prepared and this history may include psychological testing and evaluation. This type of information, information which in one sense distinguishes a juvenile from an adult court, is most difficult to computerize because it is often subjective and intuitive, not readily quantifiable and, if quantified, it often becomes extremely misleading. The problem here has been aptly stated by a Canadian Commission:

> Computers are most efficient when dealing with information that can be quantified and systemized; information that is intuitive, ambiguous, or emotional is much more difficult to computerize. As a consequence, computers may reinforce the importance in the decision-making process of the technocrat over the humanist, the objective over the subjective.[14]

The problem is demonstrated by the automated system in Worcester, Massachusetts in which the child's I.Q. is reported as a raw aggregate score, the simplest way to quantify information about intelligence. Aside from the question whether I.Q. scores should be utilized at all, reporting only the raw score raises a number of issues: it would appear to violate Ethical Standards promulgated by the American Psychological Association (Principles 14) and it is necessarily misleading because the meaning of an I.Q. score can not be understood unless the specific I.Q. test utilized is reported, the score is interpreted, at least in terms of standard deviations, and the relationship between verbal and performance scores and other information that is available about the child is explained[15] so that I.Q. can be understood in its proper context.

A third reason that I am concerned about the emerging trend towards automating juvenile records is that the records are often of poor quality, information is often collected and not used or if used it is questionable whether it should be used for that purpose. The recent observations of Edwin M. Lemert bear repeating here: "Juvenile court records . . . are inadequate or incomplete as reports; they are uneven in their description and analysis of various aspects of the minor's problem and situation. . . ."[16] Lemert also reports, "the existence of a vast amount of information in juvenile records, replete with numerous duplicates, which is seldom if ever used" and further that there is a "lack of discernable correspondence between the contents of records and recommendations made for disposition of cases."[17] Therefore, "to grasp how decisions are made . . . , one must 'read between the lines' of records or solicit informal explanations from parties involved."[18]

If Lemert's conclusions about juvenile records are accurate, and I can add that my observations of records in Massachusetts, Arizona and Nevada confirm his statements, then a discussion of computerizing juvenile records, other than for routine administrative purposes, can not be meaningful. Rather, the first step must be to analyze the informational needs of the juvenile justice system and the ability of the system to collect and use that information. Once such an analysis is undertaken we can then talk about the best form of storing that information and ask whether automation serves or disserves the information needs of the juvenile courts.

The fourth reason that I would suggest we pause before putting the juvenile justice system on the "computer bankwagon" is that first there must be a thorough examination of the laws and policies pertaining to the confidentiality of juvenile records. The need for such an examination before, rather than after computers are utilized in the juvenile courts, becomes evident from comparing the various state laws that now exist and from analyzing recent court decisions. The analysis that follows proceeds from the assumption that confidentiality is a desirable goal of the juvenile justice system.[19]

Analysis Of State Legislation

Virtually every state has enacted legislation to limit public access to juvenile court records and to declare that an adjudication of delinquency is not a conviction of a crime. The purpose of such legislation is to enhance the chances of rehabilitation by reducing the risks of collateral disabilities attaching to the disclosure of a conviction. This is a lofty purpose but, as many studies have indicated,[20] it hasn't

[10] *See,* Westin, A.F., *Data Banks in a Free Society,* 47–64 (1972).

[11] Letter from Governor Francis W. Sargent to Attorney General Elliot L. Richardson dated June 13, 1973.

[12] The risk of wholesale exposure of automated records is discussed at great length by Professor Arthur Miller in *The Assault on Privacy* (1971).

[13] The premise that juvenile courts focus on the child and not what he did may be validated by looking at almost any juvenile file and seeing that at most one page is devoted to what the child did while many pages are devoted to his "social history." Moreover, I would guess that at most only two to five percent of all juveniles who have contact with the juvenile justice system ever see an adjudication hearing since most juveniles are either diverted prior to a hearing or plead guilty.

[14] *Privacy and Computers,* A Report of a Task Force established by the Department of Communications/Department of Justice (Information Canada, 1972). The importance of intuition to a clinician has been written about extensively. *See,* Sarbin, T.R., *Clinical Psychology—Art or Science?,* 6 Psychometric 391 (1941). A full discussion of the debate about the clinical method appears in Meehl, P.E., Clinical versus Statistical Prediction (1954).

[15] *See,* McCarthy, D., *Ethical and Professional Considerations* in Reporting of Test Information 26–31 in Barnett, W.L., *Readings in Psychological Tests and Measurements* (1964). *See also,* Anastasi, A., *Psychology, Psychologists, and Psychological Testing,* 22 Amer. Psychol. 297–306 (1967).

[16] Lemert, E.M., *Records in the Juvenile Court in On Record: Files and Dossiers in American Life,* 355 (1969).

[17] *Id.* at 357.

[18] *Id.* at 359.

[19] The principle that juvenile records should generally be kept confidential is based upon the notion that a record is "organized stigma" and that the juvenile justice system, to accomplish its social welfare and rehabilitative goals, must affirmatively seek to prevent or reduce stigma from attaching or at least from being communicated. *See,* Lemert, *supra* note 16 at pp. 373-75; Schur, Radical Non-Intervention 118–30 (1973); Schwartz and Skolnick, Two Studies of Legal Stigma, 10 Social Problems 133 (1968).

[20] E.g., Miller, H.S., *The Closed Door* (1972); Sparer, E., *Employability and the Juvenile Arrest Record* (1966).

worked.[21] It hasn't worked because many employers and educators believe that they are taking risks when they employ or enroll a person with a record; because many employers and educators are unwilling to expend funds to conduct a complete investigation to determine whether the existence of a record actually reflects upon the person's present qualifications or trustworthiness, and because there are many loopholes and inadequacies in the laws which seek to preserve confidentiality and eliminate collateral disabilities.

The inadequacy of present laws pertaining to information systems in the juvenile justice system is indicated by an examination of the present state laws. Perhaps the most telling revelation from such an examination is that generally there is no formal regulation, either by statute or rule, in a number of significant areas. First, there are no laws defining the purposes for which information may legitimately be collected and utilized. Instead, it becomes apparent that the juvenile justice system assumes that so long as a court has jurisdiction, it may collect any and all information (no matter how private), and it may use that information for any purpose, subject of course to the court's own internal and subjective notions of relevancy, utility and the best allocations of resources.[22]

Second, there are no laws establishing any quality controls with regard to practices of collecting and using information. Thus, juvenile courts are not compelled to be introspective about their information-gathering practices. In other words, juvenile courts are never required to ask themselves (never mind prove) why, in a robbery case, for example, there is or is not a justification for expending resources to collect information regarding the child's performance in school or the degree to which his family is functional or dysfunctional. Then, assuming there is a justification for collecting such information, the courts are not required to ask themselves how that information is relevant to a particular decision. Instead, the courts are permitted to assume that a poor school record on a dysfunctional family is evidence of delinquency proneness — justifying intervention. But, does evidence of a poor school record or a dysfunctional family in fact warrant intervention? The answer is that we don't know. As Gottfredson has stated: "Despite the painstaking studies, item analyses and validation studies . . . , all currently available prediction methods still have only relatively low predictive power."[23] Thus, to rely upon any particular datum or combination of data to make a judgment of delinquency proneness will necessarily result in gross overpredictions. The question whether, or the extent to which, the juvenile justice system should be permitted to overpredict raises policy questions on one level. The policy question on the level of information systems is to what extent should the juvenile courts be allowed to collect and store information, particularly information of a private nature, which has a relatively low predictive power.

Third, there are no laws which presently recognize that a juvenile court's thirst for information should be weighed against a juvenile's right and need for privacy. This means that the juvenile justice system assumes that once it obtains jurisdiction over a child it may collect any and all information, no matter how "private" that information may be, no matter whether that information is only marginally relevant to a particular decision, and no matter how limited the scope of that decision may be. In addition, there is no concept of proportionality with respect to information gathering. By that I mean that the system assumes that it may gather any and all information — no matter how "private" — irrespective of whether the child is charged with a curfew violation or murder. In other words, the juvenile justice system does not start from the premise, as I would suggest it should, that a child has a right of privacy and that the justification for invading that privacy — the state's interest in intruding — should depend both upon the seriousness of his misconduct and the validity of collecting the information for a particular decision.[24]

A fourth and final area which I will mention, in which there are presently no state laws, are laws regulating the use of computers in the juvenile courts. The general need for such laws is the subject of Arthur Miller's book. *The Assault on Privacy,* and it is a subject to which Project SEARCH has given some attention. Certainly, juvenile courts must address the many legal questions which arise. The most obvious questions relate to the application of theft laws to situations in which a person obtains information from a computer without authority, the effect of computer use upon a juvenile's right of privacy and the special needs of children to be protected against the misuse of information. For purposes of this paper and this symposium, however, I only want to emphasize that computers, in one sense, simply provide a mechanism for storing, ordering and disseminating information, and meaningful analysis of that mechanism or any mechanism can only be considered in the broader context of the purposes of collecting and using information in the juvenile justice system.

Now that I have outlined what subjects, pertaining to juvenile information systems, are not the subject of formal regulation, I now turn to those issues which have been attended to by the legislatures of some states.

Only 24 states (Alaska, Connecticut, Georgia, Hawaii, Idaho, Illinois, Indiana, Kentucky, Kansas, Maryland, Minnesota, Missouri, New Mexico, North Dakota, New York, Oklahoma, Oregon, South Carolina, South Dakota, Tennessee, Utah, Vermont, Wisconsin and Wyoming) control and limit access to juvenile records in the possession of police. Therefore, the decision whether to disseminate juvenile records in the remaining 26 states is left to the discretion of each police department in each state. The laws in those states that have enacted legislation pertaining to police juvenile records are sometimes very general, as in Wyoming (§14-15.41), where it is provided that police records on juveniles must be kept separate from those of adults and that such records are confidential but may be disseminated with the consent of a judge. In Vermont (§ 663), however, the legislation is somewhat more specific and inspection is limited to specific agencies: the juvenile court, an agency to which a juvenile is committed, corrections, a criminal court for sentencing, the parole board and to other police agencies. The Iowa Code (§ 232.56), an anomaly, requires police to keep their juvenile records open to the public.[25]

Only 23 states (Connecticut, Florida, Georgia, Hawaii, Idaho, Indiana, Illinois, Kansas, Kentucky, Minnesota, Missouri, New Jersey, North Dakota, Ohio, Oklahoma, Oregon, South Carolina, Tennessee, Utah, Vermont, Virginia, Washington and Wyoming) regulate the fingerprinting and photographing of juveniles. Illinois (ch. 373 § 702–8) prohibits police from forwarding juvenile prints and photos to the F.B.I. and to the central state depository; South Carolina (ch. 15-1281.20) prohibits the fingerprinting and photographing of juveniles without judicial consent; and Florida (ch. 39.03) limits fingerprinting and photographing to felony cases, limits access to police, the juvenile court and the juvenile, and requires destruction of such records at age 21.

Only 16 states (Alaska, Arizona, California, Colorado, Connecticut, Florida, Georgia, Indiana, Missouri, New Jersey, Oklahoma, Oregon, Tennessee, Utah, Virginia and Washington) have laws

[21] *See also,* Justice Fortas' statement in *In Re Gault,* 387 U.S. 1, 24–25 (1967), to the effect that many police departments regularly supply record information to the Armed Services, social service agencies, and employers.

[22] The assumption that businesses want, need and can use more information is challenged by Ackoff, R.L., in an article entitled Management Misinformation Systems, 14 Management Science B–147 (1967).

[23] Gottfredson, D.M., Assessment and Prediction Methods in Crime and Delinquency in The President's Commission on Law Enforcement and Administration of Justice, *Task Force Report: Juvenile Delinquency and Youth Crime 171, 181* (1967). *See also,* Schur, E.M., *Radical Non-Intervention* 46-51 (1973).

[24] Two recent cases suggest the concept of proportionality although neither case arises in the juvenile court context. In *Merriken v. Cressman,* 42 U.S.L. Wk. 2203 (Gen. Law, October 16, 1973) the court held that information could not be collected for a school's drug prevention program because the information sought was of a private nature and was not shown to be sufficiently relevant to the purposes for which it would be used. *See also Wentworth v. Schlesinger,* 42 U.S.L. Wk. 2271 (Gen. Law, November 27, 1973).

[25] Query whether an employer in Iowa would have the right to have access to the police computer to secure printouts of all juveniles with an arrest record.

providing for juvenile records to be destroyed.[26] The Connecticut statute, (§ 17–72a), authorizing destruction of records, requires the immediate "erasure" of all police and court records if the child is found not delinquent and the "removal" of "all references" to the case if the child was found delinquent and is not charged with a subsequent offense for two years thereafter. California, in addition to a statute authorizing the sealing of records (Welf. and Instit. Code § 781), gives each juvenile court the power to destroy records other than the docket and minute book. (Welf. and Inst. Code § 826). Missouri law (title 12 § 211.32) on this point is similar to California, while New Jersey excludes from its "expungement" statute certain designated serious crimes.

Six states (Alaska, Colorado, Maine, New Mexico, South Carolina, and Vermont) and the District of Columbia make it a crime to improperly disclose juvenile record information; but it is not a crime in the other states to disclose juvenile records to unauthorized persons. The District of Columbia Code (§ 11–1586) makes it a crime to disclose, use or receive juvenile record information without authority; the Alaska criminal statute (ch. 47.10.090) is limited to unauthorized disclosure by the news media; and the Maine code (ch. 15 § 2609) makes it criminal contempt to divulge matters before the juvenile court.

Nine states (Connecticut, California, Kentucky, New Mexico, Ohio, Oregon, Utah, Vermont and Wyoming) provide that once a juvenile record is sealed, the proceedings "shall be deemed never to have occurred;" the other states have no similar provision. The practical effect of such a provision is to authorize a juvenile to answer an employer, credit company, etc. that he has no record. See, e.g., Cal. Welf. and Inst. Code § 781. By contrast, a juvenile in another state, even if his record is sealed, does not have the legal right to deny the existence of a juvenile record (although the Court or Probation Office may have the authority to do so) and he would in fact be required to disclose the existence of a record in an application for public employment which had to be signed under the penalties of perjury. Even if local law provides that the public employer may not deny the applicant a job merely because he has a juvenile record (e.g., Mass. Gen. Laws ch. 119 § 60) it has been held that the employer may refuse the job based, not upon the record itself, but the underlying facts of the case. See, *Cacchiola v. Hoberman*, 31 N.Y.2d 287, 291 N.E.2d 117 (1972) (concurring opinion). But see, *TNG v. Superior Court*, 94 Cal. Rptr. 813, 484 P.2d 981 (1971). Thus, it can be seen that the failure to authorize a juvenile to deny the existence of record, and the failure to prohibit an employer from asking about a record, establishes a loophole and an opportunity to deny benefits to juveniles.[27]

Only seven states (Florida, Georgia, Hawaii, Idaho, New Mexico, South Dakota and Utah) have laws which specifically regulate access to juvenile records by researchers. A typical provision with respect to research access, Georgia Code § 24A–3501, limits research to "authorized representatives of recognized organizations compiling statistics for proper purposes" and requires judicial approval. In Utah (§ 55–10–116), the law merely states that a judge "may" provide access to "persons conducting pertinent research studies" and by implication prohibits researchers from having access to probation records. Compare, North Dakota Code § 27–20–51 which does not specifically refer to access by researchers but does permit the court to "disclose" records to named persons, including "any other person having a legitimate interest . . . in the work of the court;" presumably this provision is designed to govern research access.

Only six states (Alaska, Colorado, Georgia, Maine, Montana and South Carolina) have laws which prohibit the news media from publishing the names or photo of a juvenile. In Montana, the limitations on publication apply only to nonfelony charges (ch. 10–633). In Mississippi a contrary policy exists: the name of the juvenile and the names of his parents must be published in a local newspaper if the juvenile is a second offender.

Only 11 states (Alaska, Connecticut, Florida, Georgia, Idaho, Hawaii, Iowa, Kentucky, Louisiana, Oregon and South Carolina) have statutes which provide that information contained in juvenile records is privileged. In Alaska (§ 47.10.090), the Code expressly states that the information is "privileged" while in states such as Connecticut (§ 571–84) a privilege is created by implication: "no information . . . shall be disclosed directly or indirectly." Some other states, such as Massachusetts, have laws making record information inadmissible as evidence in court (ch. 119 § 60; ch. 120 § 21). The practical distinction between privilege and evidentiary laws is that the evidentiary rule usually applies only to "courts" and thus, a probation officer could theoretically be compelled to testify before an administrative agency or any other non-court investigative agency.

Finally, a number of states provide that a juvenile or his attorney have a right of access to the juvenile's probation report (Colorado, Minnesota, New Mexico, Oregon, South Carolina, Tennessee, Washington, Wyoming, Connecticut, Georgia, and North Dakota). Although it appears to be nearly a universal practice [28] to allow the attorney for a juvenile to inspect a probation officer's records, most states do not have laws which compel that result and, therefore, the privilege of access may be denied if the juvenile's attorney and the probation office are not on good terms.

To summarize, most states have laws which serve as a general declaration that persons should not be denied opportunities based upon a juvenile record. But, most states do not have laws which are specific enough to assure that the general legislative purpose is likely to become a reality. However, an examination of the laws of all the states reveals many provisions which may serve as a basis for the kinds of regulation which is needed. These are laws:

1. Regulating dissemination of police records;
2. Regulating fingerprinting of photographing;
3. Permitting or requiring the destruction of records;
4. Requiring the sealing of records;
5. Making it a crime to disclose juvenile records;
6. Providing that a juvenile proceeding is "deemed not to have occurred" once the record is sealed; [29]
7. Regulating access by researchers;
8. Regulating access by the media;
9. Creating a privilege with respect to juvenile record information;
10. Giving juveniles or their attorneys access to probation records.

The enactment of legislation in all of the above areas does not, of course, exhaust all of the possibilities for protecting information pertaining to juveniles. Enactment of such legislation would, however, provide a much firmer foundation to protect juvenile records and if combined with legislation focusing upon standards for collecting information, referred to earlier in this section, the risk of misuse of information would be substantially reduced.

Analysis of Relevant Case Law

Historically, the decision to collect, retain and

[26] Eleven states (California, Kentucky, Maryland, Massachusetts, New Mexico, North Dakota, Ohio, South Dakota, Utah, Vermont and Wyoming) have laws providing that, under certain circumstances, juvenile records may be sealed. Since the functional effect of sealing records is to close them to the public and juvenile court records are theoretically closed anyway, sealing statutes give a juvenile little added protection. If, however, police records are sealed with the court records, the effect of sealing may be beneficial to a juvenile. But *see*, Kogon and Loughery, *Sealing and Expungement of Criminal Records—The Big Lie*, 61 J. of Crim. L. and Police Science 378 (1970) in which the authors refer to sealing and expungement statutes as a hoax.

[27] It is perhaps logical to assume that states which have fully accepted the philosophy of confidentiality would prohibit employers, credit companies, etc. from inquiring about either the existence of a juvenile record or the underlying facts of a juvenile offense. Whether that would be a good philosophy in all cases is subject to debate. Gough, The Expungement of Adjudication Records, 1966 Wash. U.L.Q. 147, 178–86.

[28] A 1963 survey reported that two-thirds of the judges surveyed regularly supplied probation reports to the attorneys and only five percent never did so. Skoler, D.L. and Tenney, C.W., *Attorney Representation in Juvenile Court*, 4 Journal of Family Law 77, 86–87 (1964). Both the Uniform Juvenile Court Act and the Legislative Guidelines of the Children's Bureau include rules which would accord attorneys access to all juvenile records.

[29] It has been argued that it is hypocritical and perhaps inconsistent with the philosophy of the juvenile courts to permit, either by legislative enactment or by court rule, a juvenile to lie by denying that he has ever had a record when in fact a record has existed. This argument was made and rejected in *T.N.G. v. Superior Court*, 4 Cal. 3d 767 (1971).

release record information has been regarded as exclusively within the discretion of each criminal justice agency.[30] A number of recent cases indicates, however, that the judiciary is now willing to promulgate standards pertaining to the practice of maintaining arrest records in certain cases. For the most part, those decisions have focused upon unusual facts.[31] However, other cases have broadly examined both the law enforcement need to retain arrest records and the harm caused by dissemination and have concluded that at least in cases where there has been an acquittal and there has been no affirmative showing of the need to retain the record, expungement will be required.[32] The legal premise of these cases has been either that the retention of an arrest record without proof of a compelling state purpose to support retention is an invasion of the constitutional right of privacy [33] or that expungement may be an appropriate remedy to redress a constitutionally unlawful arrest.[34]

The recent cases in which courts have broadly construed the right of expungement do not necessarily mean, however, that courts will be willing to carefully scrutinize the legitimacy of a law enforcement purpose that is asserted in support of the release of a record. For example, in the recent case of *Tosh v. Buddies Supermarkets*,[35] the police released the conviction records and "mug shots" of union organizers to a supermarket that was in the process of resisting a campaign to unionize its employees. The union organizers sought an injunction and damages when the supermarket published the "rap sheets" on 14×20 inch posters. The court denied the claim finding a "legitimate need" for the release because the supermarket could be "better prepared to deal with" conduct which might be threatening to customers or store employees.

Although the cases that are discussed above involve adult criminal records and not juvenile records, it is reasonable to conclude that most courts would apply similar reasoning to a case involving a juvenile. Indeed, courts have held that expungement of juvenile records may be ordered in cases where there has been an acquittal relying upon the broad policies of confidentiality and rehabilitation expressed in a state's Juvenile Court Act.[36]

One very recent case, *Merriken v. Cressman*,[37] substantially extends the right of juveniles to be protected from stigmatizing labels. In that case, the court found that a program established by a school district to identify potential drug abusers in the eighth grade violated the children's constitutional right of privacy in that the information collected was of a private nature and not shown to have any necessary use for drug abuse prevention, there were not adequate protections to assure the confidentiality of the information, and the risks of harm from mislabeling or misuse were regarded as too significant to permit collection and retention of the information.

In summary, although courts are just beginning to analyze the right of criminal justice agencies to retain juvenile records, it is likely that the courts will at least adopt the following principles generally:

1. All records must be expunged if a juvenile has been arrested without probable cause and the charges are subsequently dismissed.
2. All records must be expunged if a juvenile's case is dismissed or there is a finding of not guilty unless it can be shown that the records are not disseminated *and* that their retention is necessary for some valid law enforcement purpose.
3. All records must include the disposition of the case.

Interestingly, only Connecticut presently has a statute which compels compliance with the first two principles and no states have a law to assure compliance with the third.

Conclusion

Before a juvenile court begins to plan to introduce automation into its record keeping practices, for other than routine administrative matters (such as collecting aggregate data, docket control or providing information about community placements and programs), it is necessary to first examine the juvenile court's informational needs, how it collects and uses information, how information can stigmatize children in unintended ways, the laws pertaining to the confidentiality of juvenile records and the special problems related to reducing clinical information to a format from which it may be converted into an automated system. Once such an analysis is completed, it is very likely that the conclusion will be that much of the information that is presently collected by juvenile courts is irrelevant or is not used and the most pertinent information cannot be reduced to a computer format and retain its meaning. In addition, while present laws pertaining to the confidentiality of information are inadequate, and appropriate amendments can be made to substantially reduce the risk of improper disclosure and misuse of information, the best protection against stigmatizing children, if that is to continue to be a primary goal of the system, is not to collect information for purposes of creating a record unless it is absolutely needed for purposes which are evident. In any case, it is hoped that we will not spend millions of dollars on hardware and software, instead of spending it on services for children, without at least asking ourselves why we want the information in the first place and once we get it how we should and can use it.

[30] E.g., *Fernicola v. Kennan*, 39 A.2d 851 (N.J. Chan. 1944).

[31] *See, Hughes v. Rizzo*, 282F. Supp. 881 (E.D. Penn. 1968) (police conducted clearly illegal mass arrests to clear park of hippies—arrest records ordered expunged); *Sullivan v. Murphy*, 41 U.S.L.Wk. 2598 (Gen. 5/15/73) (mass arrests without probable cause during May day demonstration—arrest records ordered expunged); *Bilick v. Dudley*; — F. Supp. — (S.D.N.Y. No. 67 Civ. 3317, 3/30/73) (mass arrest without probable cause to break up political rally—court records ordered expunged).

[32] *See, Eddy v. Moore*, 5 Wash. App. 334, 487 P.2d 211 (1971); *Davidson v. Dill*, —Colo—, 503 P.2d 157 (1972). See also, *Menard v. Mitchell*, 430 F.2d 486 (D.C. Cir. 1970).

[33] *Eddy v. Moore, supra.*

[34] *Menard v. Mitchell, supra* at 491.

[35] 482 F.2d 329 (5th Cir. 1973).

[36] See, *In Re Smith*, 63 Misc. 2d 198 (1970); *Henry v. Looney*, 65 Misc. 2d 759 (1971); *Coffee, Privacy versus Parens Patriae*, 57 Cornell L. Rev. 571 (1972); Gough, The Expungement of Adjudication Records, 1966 Wash. U.L.A. 147. But see, *Dugan v. Police Dept. City of Camden*, 112 N.J. Super. 482, 271 A.2d 727 (1970) in which the court rejected a challenge of the general right of police to retain juvenile arrest records on the grounds that such police records were not open to the public and their retention is justified to permit police to perform necessary investigative and preventive activities.

[37] 42 U.S.L. Wk. 2203 (Gen. Law, October 16, 1973).

Appendix X

STATE OF WASHINGTON
44TH REGULAR SESSION

Senate Joint Resolution No. 123

by Senators Goltz, Fleming, Buffington, McDermott and Morrison

Read first time February 20, 1975, and referred to JUDICIARY COMMITTEE.

BE IT RESOLVED, BY THE SENATE AND HOUSE OF REPRESENTATIVES OF THE STATE OF WASHINGTON, IN LEGISLATIVE SESSION ASSEMBLED:

THAT, At the next general election to be held in this state there shall be submitted to the qualified voters of the state for their approval and ratification, or rejection, an amendment to Article I of the Constitution of the state of Washington by amending section 7 thereof to read as follows:

Article I, section 7. No person shall be disturbed in his private affairs, or his home invaded, without authority of law. **The right of privacy is hereby declared to be a fundamental right of the people.**

BE IT FURTHER RESOLVED, That the secretary of state shall cause notice of the foregoing constitutional amendment to be published at least four times during the four weeks next preceding the election in every legal newspaper in the state.

Appendix XI

STATE OF NEW YORK

1975–1976 Regular Sessions

In Assembly

January 8, 1975

Introduced by Mr. CULHANE—Multi-sponsored by—Messrs. STRELZIN, DiFALCO, BREWER, GRIFFITH, MONTANO, FERRIS, GRABER, HARENBERG, STOTT, LEVY, D'AMATO, DELLI BOVI, MOLINARI, O'NEIL, SULLIVAN, DEARIE, WALSH, SERRANO—read once and referred to the Committee on Commerce, Industry and Economic Development—reference changed to Committee on Consumer Affairs and Protection—committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee—reported from said committee with amendments, ordered reprinted as amended and placed on the order of second reading—passed by Assembly and delivered to the Senate—recalled from Senate, vote reconsidered, bill amended, ordered reprinted and restored to third reading.

AN ACT

to amend the general business law, in relation to consumer credit reporting

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. The legislature hereby finds and declares:

(1) The banking system is dependent upon fair and accurate credit reporting. Inaccurate credit reports directly impair the efficiency of the banking system, and unfair credit reporting methods undermine the public confidence which is essential to the continued functioning of the banking system.

(2) An elaborate mechanism has been developed for investigating and evaluating the credit worthiness, credit standing, credit capacity, character, and general reputation of consumers.

(3) Consumer reporting agencies have assumed a vital role in assembling and evaluating consumer credit and other information on consumers.

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

(5) It is the purpose of this article to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this article.

In furtherance of these findings the legislature does enact this article.

§ 2. The general business law is hereby amended by inserting therein a new article, to be article twenty-five-A, to read as follows:

ARTICLE 25-A

FAIR CREDIT REPORTING ACT

§ 380. Short title. This article may be cited as the fair credit reporting act.

§ 380–a. Definitions. (a) The term "person" means any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity.

(b) The term "consumer" means an individual.

(c) The term "consumer report" means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation,

personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (1) credit or insurance to be used primarily for personal, family, or household purposes, or (2) employment purposes. The term does not include (i) any report containing information solely as to transactions or experiences between the consumer and the person making the report or (ii) any authorization or approval of a specific extension of credit directly or indirectly by the issuer of a credit card or similar device.

(d) The term "investigative consumer report" means a consumer report or portion thereof in which information on a consumer's character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on or with others with whom he is acquainted or who may have knowledge concerning any such items of information. However, such information shall not include specific factual information on a consumer's credit record obtained directly from a creditor of the consumer or from a consumer reporting agency when such information was obtained directly from a creditor of the consumer or from the consumer.

(e) The term "consumer reporting agency" means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports or investigative consumer reports to third parties.

(f) The term "file" when used in connection with information on any consumer, means all of the information on that consumer recorded and retained by a consumer reporting agency regardless of how the information is stored.

(g) The term "employment purposes" when used in connection with a consumer report means a report used for the purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee.

(h) The term "merchant" means any person who receives a consumer report or investigative consumer report from a consumer reporting agency or who provides information to a consumer reporting agency pursuant to a contract or for a fee, or who otherwise regularly provides information to a consumer reporting agency.

(i) The term "adverse information" means information that is likely to have a negative effect upon the ability or eligibility of a consumer to obtain credit, credit insurance, employment, or other benefits, goods or services.

(j) The term "user" when discussed in connection with the use of a consumer report means any recipient of a consumer report or an investigative consumer report other than the subject thereof.

§ 380–b. Permissible dissemination of reports. A consumer reporting agency may furnish a consumer report under the following circumstances and no other:

(a) In response to the order of a court having jurisdiction to issue such an order.

(b) In accordance with the written instructions and authorization of the consumer to whom it relates.

§ 380–c. Preparation and/or procurement of consumer reports. (a) A person may not procure or cause to be prepared a consumer report on any consumer unless such person has provided the consumer with clear and conspicuous written notice of the requested procurement or preparation and the consumer has, in turn, given a specific, dated, and separately signed written authorization for each preparation or procurement.

(b) The notice to the consumer, which is required by the preceding subdivision: (1) must inform the consumer of the names, addresses, and telephone numbers of any and all consumer reporting agencies that will be requested to prepare or disseminate consumer reports about the particular consumer, and (2) must clearly and conspicuously inform the consumer that he may request and receive from all such consumer reporting agencies copies of any and all such consumer reports.

§ 380–d. Preparation and/or procurement of investigative consumer reports. (a) A person may not procure or cause to be prepared an investigative consumer report on any consumer unless such person has provided the consumer with clear and conspicuous written notice of the requested procurement or preparation and the consumer has, in turn, given a specific, dated, and separately signed written authorization for each preparation or procurement.

(b) The notice to the consumer, which is required by the preceding subdivision: (1) must inform the consumer of the names, addresses, and telephone numbers of any and all cousumer reporting agencies that will be requested to prepare or disseminate consumer reports about the particular consumer; (2) must clearly and conspicuously inform the consumer that he may request and receive from all such consumer reporting agencies copies of any and all such investigative consumer reports; (3) must provide a list of all questions to be asked in the investigation and the likely sources to be contacted in the investigation; and (4) must provide a blank copy of any standard questionnaire or other similar form to be used in the investigation.

§ 380–e. Disclosures to consumers. (a) Every consumer reporting agency shall, upon request and proper identification of any consumer, clearly and accurately disclose to the consumer:

(1) all information in its files on the consumer at the time of the request;

(2) the sources of the information;

(3) the recipients of any consumer report or investigative consumer report on the consumer which it has furnished:

(i) for employment purposes within the two-year period preceding the request, and

(ii) for any other purpose within the six-month period preceding the request.

(b) The requirements of subdivision (a) respecting the disclosure of source of information and the recipients of consumer reports do not apply to information received or consumer reports furnished prior to the effective date of this article except to the extent that the matter involved is contained in the files of the consumer reporting agency on that date.

§ 380–f. Methods and conditions of disclosure to consumers. (a) A consumer reporting agency shall make the disclosures required under section three hundred eighty-e during normal business hours and on reasonable notice.

(b) The disclosures required under section three hundred eighty-e shall be made to the consumer by one or more of the following methods:

(1) in person if he appears in person and furnishes proper identification, and in any such case the consumer shall be permitted a personal visual inspection of his file; or

(2) by telephone if he has made a written request, with proper identification, for telephone disclosure and the toll charge, if any, for the telephone call is prepaid by or charged directly to the consumer. In the event the telephone call is made after an adverse consumer determination, the cost of such call shall be paid by the consumer reporting agency; or

(3) by mailing a copy of the consumer's file to him, if he has made a written request with proper identification, at a charge for photocopying not to exceed ten cents per page. In the event that the request for a copy of the consumer's file is made after an adverse consumer determination, the cost of such disclosure shall be paid by the consumer reporting agency.

(c) Any consumer reporting agency shall provide trained personnel to explain to the consumer any information furnished to him either by personal interview or telephone communication, and information furnished by mail must be accompanied by an explanation of such information if provided in code or trade terminology.

(d) The consumer who seeks disclosure by means of a personal interview pursuant to paragraph (1) of subdivision (b) of this section shall be permitted to be accompanied by one other person of his choosing, who shall furnish reasonable identification. A consumer reporting agency may require the consumer to furnish a written statement granting permission to the consumer reporting agency to discuss the consumer's file in such person's presence.

§ 380–g. Procedure for correcting inaccurate, irrelevant and misleading information. (a) A consumer reporting agency shall adopt reasonable procedures to enable a consumer to correct any inaccurate, irrelevant or misleading information in his file.

(b) If a consumer disputes any item of information contained in his file on the ground that it is inaccurate, irrelevant or misleading, and such dispute is directly conveyed to the consumer reporting agency by the consumer, the consumer reporting agency shall promptly re-investigate and record the current status of such information, unless it has reasonable grounds to believe that the dispute by the consumer is frivolous, and it shall promptly notify the consumer of the result of its investigation and his rights pursuant to subdivisions (d), (e) and (f) of this section. The presence of contradictory information in a consumer's file shall not, in and of itself, constitute reasonable grounds for believing the dispute is frivolous.

(c) Upon re-investigation the consumer reporting agency shall record in the consumer's file the efforts undertaken to re-investigate the dispute, including but

not limited to the names of the person or persons conducting the re-investigation, and the names of the persons who provided information in connection with the re-investigation.

(d) If, after conducting the re-investigation prescribed by subdivision (b) of this section, the consumer reporting agency finds that an item is in error or that it can no longer be verified, it shall: (1) promptly expunge the item and otherwise correct the file, (2) refrain from reporting the item in subsequent consumer reports, and (3) promptly notify all persons who have received information regarding the item during the previous two years that an error existed and furnish them with the corrected information.

(e) If, after conducting the re-investigation prescribed by subdivision (b) of this section, the consumer reporting agency is unable to resolve any difference still remaining between the allegations made by its sources and the consumer, it shall, (1) promptly indicate in the file that the item is disputed, (2) permit the consumer to file a statement containing the nature of the dispute; the agency may limit such statements to not more than one hundred words if it provides the consumer with assistance in writing a clear summary of the dispute, (3) include the consumer's statement of the dispute in all subsequent credit reports containing the information in question, and (4) clearly note in all subsequent consumer reports that the item is disputed by the consumer.

(f) Following any deletion of information which is found to be inaccurate or the accuracy of which can no longer be verified or any notation as to disputed information, the consumer reporting agency shall furnish notification that the item has been deleted and include a copy of the consumer's statement, where applicable, in accordance with subdivision (e) of this section, to any person who has received a consumer report within two years prior thereto.

§ 380–h. Public record information for employment purposes. A consumer reporting agency which furnishes a consumer report for employment purposes and which for that purpose compiles and reports items of information on consumers which are matters of public record and are likely to have an adverse effect upon a consumer's ability to obtain employment shall:

(a) At the time such public record information is reported to the user of such consumer report, notify the consumer of the fact that public record information is being reported by the consumer reporting agency, together with the name and address of the person to whom such information is being reported; or

(b) Maintain strict procedures designed to insure that whenever public record information which is likely to have an adverse effect on a consumer's ability to obtain employment is reported it is complete and up to date. For purposes of this subdivision, items of public record relating to convictions, suits, tax liens, and outstanding judgments shall be considered up to date if the current public record status of the item at the time of the report is reported.

§ 380–i. Restrictions on investigative consumer reports. (a) Whenever a consumer reporting agency prepares an investigative consumer report, no adverse information in the consumer report (other than information which is a matter of

public record) may be included in a subsequent consumer report unless such adverse information has been verified in the process of making such subsequent consumer report, or the adverse information was received within the three-month period preceding the date the subsequent report is furnished.

(b) Each investigative consumer report shall be in writing, shall identify the sources of all information contained therein, and shall be retained in the file of the consumer to whom it relates for a period of one year following its completion.

§ 380–j. Requirements on users of consumer reports. (a) Whenever any adverse action is taken either wholly or partly because of information contained in a consumer report or partly because of information contained in a consumer report from a consumer reporting agency, the user taking such action shall:

(1) disclose in writing to the consumer against whom such adverse action has been taken (i) the reason for taking such adverse action, including reference to the particular item or items of information contained in the consumer report upon which such adverse action has been wholly or partly based; (ii) the name, street address, and telephone number of the consumer reporting agency making the report; and (iii) a statement of the fact that the consumer is entitled to obtain the specific methods of disclosure of his file provided for in section three hundred and eighty-f; and

(2) furnish a copy of the consumer report if the consumer report was written, or furnish a copy of a summary if the consumer report was oral.

(b) Whenever credit or insurance for personal, family, or household purposes, or employment involving a consumer is denied or the charge for such credit or insurance is increased either wholly or partly because of information obtained from a person other than a consumer reporting agency bearing upon the consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, the user of such information shall disclose in writing to the consumer at the time such action is taken the reason for such adverse action, and the nature of the information.

(c) Whenever a user or potential user of consumer reports procures or causes to be prepared a consumer report on any consumer, such user or potential user shall be required to comply with the requirements of this article.

(d) Every user of a consumer report or an investigative consumer report shall be prohibited from disseminating any such report to any other person.

§ 380–k. Prohibited information, accuracy, relevancy and obsolescence of information in reports. (a) Neither a consumer reporting agency nor a merchant shall collect, evaluate, prepare, use or report information which is not reasonably relevant to the purpose for which it is sought.

Neither a consumer reporting agency nor a merchant shall collect, evaluate, prepare, use or report information relative to an arrest or a criminal conviction for such offense, or information based on uncorroborated hearsay, or information about a consumer's race, religion, color, ancestry, ethnic origin, personal life style, philosophy, or political affiliation.

(b) Neither a consumer reporting agency nor a merchant shall collect, evaluate, prepare, use or report information which is obsolete or which it has reason to know is inaccurate or irrelevant.

(c) A consumer reporting agency and a merchant shall adopt and follow reasonable procedures designed to (1) assure maximum possible accuracy of the information concerning the individual about whom the report relates, (2) verify the accuracy and the relevancy of such information, and (3) exclude inaccurate and irrelevant information from their files.

(d) (1) Except as authorized under paragraph two of this subdivision, no consumer reporting agency may make any consumer report containing any of the following items of information:

(i) bankruptcies which, from date of adjudication of the most recent bankruptcy, antedate the report by more than fourteen years.

(ii) suits and judgments which, from date of entry, antedate the report by more than seven years or until the governing statute of limitations has expired, whichever is the longer period.

(iii) paid tax liens which, from date of payment, antedate the report by more than seven years.

(iv) accounts placed for collection or charged to profit and loss which antedate the report by more than seven years.

(v) records of conviction of crime which, from date of disposition, release, or parole, antedate the report by more than seven years.

(vi) information regarding drug or alcoholic addiction where the last reported incident relating to such addiction antedates the consumer report or investigative consumer report by more than seven years.

(vii) information relating to past confinement in a mental institution where the date of last confinement antedates the report by more than seven years.

(viii) any other adverse item of information which antedates the report by more than seven years.

(2) The provisions of paragraph one of this subdivision are not applicable in the case of any consumer credit report to be used in connection with:

(i) a credit transaction involving, or which may reasonably be expected to involve a principal amount of fifty thousand dollars, or more;

(ii) the underwriting of life insurance involving, or which may reasonably be expected to involve, a face amount of fifty thousand dollars or more;

(iii) the employment of any individual at an annual salary which equals, or which may reasonably be expected to equal twenty-five thousand dollars, or more;

(e) No consumer reporting agency shall issue a consumer report which lists a person as having been denied credit if the sole reason for such denial is lack of

sufficient information to grant credit, unless the report states that the denial was for such reason.

§ **380-l. Civil liability for willful noncompliance.** Any consumer reporting agency or user of information which willfully and knowingly fails to comply with any requirement imposed under this article with respect to any consumer is liable to that consumer in an amount equal to the sum of:

(a) Any actual damages sustained by the consumer as a result of the failure;

(b) Such amount of punitive damages as the court may allow; and

(c) In the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

§ **380-m. Civil liability for negligent noncompliance.** Any consumer reporting agency or user of information which is negligent in failing to comply with any requirement imposed under this article with respect to any consumer is liable to that consumer in an amount equal to the sum of:

(a) Any actual damages sustained by the consumer as a result of the failure;

(b) Such amount of special damages as the court may allow, but not less than one hundred dollars for each item of erroneous information reported; and

(c) In the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

§ **380-n. Jurisdiction of courts; limitation of actions.** An action to enforce any liability created under this article may be brought in any court of competent jurisdiction, within two years from the date on which the liability arises, except that where a defendant has materially and willfully misrepresented any information required under this title to be disclosed to an individual and the information so misrepresented is material to the establishment of the defendant's liability to that individual under this article, the action may be brought at any time within two years after the discovery by the individual of the misrepresentation.

§ **380-o. Obtaining information under false pretenses.** Any person who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses shall be fined not more than five thousand dollars or imprisoned not more than one year, or both.

§ **380-p Unauthorized disclosures by officers or employees.** Any officer or employee of a consumer reporting agency who knowingly and willfully provides information concerning an individual from the agency's files to a person not authorized to receive information shall be fined not more than five thousand dollars or imprisoned not more than one year, or both.

§ **380-q. Merchant harassment.** No merchant shall threaten any consumer with consequences adverse to his credit standing by reason of a report to be made by the merchant to a consumer reporting agency. Nothing in this section shall prohibit a merchant from reporting information to a consumer reporting agency in conformity with this article.

§ **380-r. Severability.** If any provision of this article or the application thereof to any person or circumstances is held to be invalid, such invalidity shall not affect other provisions or applications of this article which can be given effect without the invalid provision or application, and to this end the provisions of this article are severable.

§ 3. Articles twenty-five-A and twenty-five-B of such law are hereby renumbered to be articles twenty-five-B and twenty-five-C, respectively.

§ 4. This act shall take effect on the first day of July next succeeding the date on which it shall have become a law.

COMMONWEALTH OF MASSACHUSETTS

House . . . . . No. 3152

January 8, 1975

By Mr. Mofenson of Newton, petition of David J. Mofenson and Chester G. Atkins for legislation to protect personal privacy by prohibiting unwarranted disclosure of personal bank and telephone records. The Judiciary.

In the Year One Thousand Nine Hundred and Seventy-Five.

AN ACT TO PROTECT PERSONAL PRIVACY BY PROHIBITING UNWARRANTED DISCLOSURE OF PERSONAL BANK AND TELEPHONE RECORDS.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

SECTION 1. Chapter 166 of the General Laws is hereby amended by inserting, after Section 15D, the following section: —

Section 15E. No telephone company doing business within the commonwealth shall divulge any information concerning any of its customers or subcribers to any individual, corporation, partnership, association, or governmental entity, except as may be required by federal law or permitted by statute of the commonwealth or except upon presentation of a proper subpoena from a court of law, upon written request of such customer or subscriber, or in order to arrange for collection of unpaid bills. Any such company which violates any provision of this section shall be liable to the customer or subscriber to whom such information relates for the greater of the following amounts: (a) one thousand dollars, plus costs and reasonable attorney fees; or (b) three times the amount of actual damages, if any, sustained plus costs and reasonable attorney fees.

SECTION 2. Section 1 of Chapter 167 of the General Laws as most recently amended by section 1 of chapter 452 of the acts of 1935, is hereby further amended by inserting, at the end thereof, the following definition: —

"Customer", an individual, partnership, corporation, firm, or association which conducts any banking transaction with a bank, including, but not limited to, opening and depositing or withdrawing funds from a savings or checking account, seeking or obtaining a loan, mortgage, or other indebtedness, making payment upon such loan, mortgage, or debt, or seeking or maintaining a credit card issued by a bank.

SECTION 3. Chapter 167 of the General Laws is hereby amended by inserting, after section 48B, the following section:—

Section 48C. No individual, partnership, association or corporation operating a bank or savings and loan association in the commonwealth shall divulge any information concerning any of its customers to any individual, corporation, partnership, association, or governmental entity, except as may be required by federal law or permitted by statute of the commonwealth or except upon presentation of a proper subpoena from a court of law, upon written request of such customer, or in order to arrange for the collection of unpaid debts. Any such individual, partnership, association or corporation which violates any provision of this section shall be liable to the customer to whom such information relates for the greater of the following amounts: (a) one thousand dollars, plus costs and reasonable attorney fees; or (b) three times the amount of actual damages, if any, sustained, plus costs and reasonable attorney fees.

SECTION 4. This act shall take effect on January first, nineteen hundred and seventy-six.

CALIFORNIA LEGISLATURE
1975-76 REGULAR SESSION

Assembly Bill . . . . . No. 1429

Introduced by Assemblyman Sieroty
(Coauthor: Senator Carpenter)

April 3, 1975

REFERRED TO COMMITTEE ON CRIMINAL JUSTICE

An act to amend Section 10145 and 10146 of the Business and Professions Code, and to repeal Section 1917 of the Financial Code, and to amend Sections 12537 and 12586 of, and add Chapter 20 (commencing with Section 7460) to Division 7 of Title 1 of, the Government Code, to add Sections 904 and 1703 to the Insurance Code, and to amend Section 11703 of the Vehicle Code, relating to financial records.

LEGISLATIVE COUNSEL'S DIGEST

AB 1429, as introduced, Sieroty (Crim.J.). Financial records: search and seizure.

Presently, the law does not provide for a special procedure to be followed when a state or local agency seeks to examine financial records, of a customer in the course of a civil or criminal investigation.

This bill enacts the "California Right to Financial Privacy Act." It provides that no officer, employee, or agent of a state or local agency, as defined, or department thereof, may request or obtain from a financial institution, as defined, copies of financial records or information from such records on any customer except in specified circumstances and by specified procedures, and limits the use of financial records authorized to be received.

This bill makes a violation of the California Right to Financial Privacy Act a misdemeanor. It authorizes injunctive relief, and reasonable attorney's fees upon successful action.

The bill requires specified persons, corporations, and licensees to authorize specified state agencies to examine various financial records as a condition of doing business, obtaining a license, or exercising privileges.

It provides that neither appropriation is made nor obligation created for the reimbursement of any local agency for any costs incurred by it pursuant to this act.

Vote: majority. Appropriation: no. Fiscal committee: no. State-mandated local program: no state funding.

The people of the State of California do enact as follows:

SECTION 1. Section 10145 of the Business and Professions Code is amended to read:

10145. A real estate licensee who accepts funds from others in connection with any transaction subject to this part who does not immediately place such funds into a neutral escrow depository or into the hands of his principal shall place such funds into a trust fund account maintained by him in some bank or recognized depository and shall retain all such funds in the account until such time as he has made a disbursement of the funds in accordance with instructions from the principal or principals in the transaction; provided that a real estate broker when acting as a principal pursuant to Section 10131.1 or Article 6 (commencing with Section 10237) of this part shall place all purchase funds for real property sales contracts or promissory notes secured directly or collaterally by liens on real property being sold by him in a neutral escrow depository unless delivery of the note or contract is made simultaneously with the receipt of the funds. A separate record shall be maintained of all moneys received subject to this section and shall further indicate the disposition thereof. Upon request of the commissioner a licensee shall furnish to the commissioner an authorization for examination of financial records of any such trust fund account, maintained in a financial institution, in accordance with the procedures set forth in Section 7473 of the Government Code.

As used in this section "neutral escrow" means an escrow business conducted by a person licensed under Division 6 (commencing with Section 17000) of the Financial Code or by any person described by subdivision (a) of Section 17006 and subdivision (c) of Section 17006 of said code.

SECTION 2. Section 10146 of the Business and Professions Code is amended to read:

10146. Any real estate broker who contracts for or collects an advance fee from any other person, hereinafter referred to as the "principal," shall deposit any such amount or amounts, when collected in a trust account with a bank or other recognized depository. Such funds are trust funds and not the funds of the agent. Amounts may be withdrawn therefrom for the benefit of the agent only when actually expended for the benefit of the principal or five days after the verified accounts mentioned hereinafter have been mailed to the principal. Upon request of the commissioner a broker shall furnish to the commissioner an authorization for examination of financial records of the trust account in accordance with the procedures set forth in Section 7473 of the Government Code.

The commissioner may issue such rules and regulations as he deems necessary to regulate the method of accounting, and to accomplish the purpose of the provisions of this code relating to advance fees including, but not limited to, establishing forms for and determining information to be included in such accountings. Each principal shall be furnished a verified copy of such accountings at the end of each calendar quarter and when the contract has been completely performed by

the licensee. The Real Estate Commissioner shall be furnished a verified copy of any account or all accounts on his demand therefor.

Where advance fees actually paid by or on behalf of any principal are not handled in accordance with the preceding paragraph, it shall be presumed that the agent has violated Sections 506 and 506a of the Penal Code. The principal may recover treble damages for amounts so misapplied and shall be entitled to reasonable attorneys' fees in any action brought to recover the same.

SECTION 3. Section 1917 of the Financial Code is repealed.

SECTION 4. Chapter 20 (commencing with Section 7460) is added to Division 7 of Title 1 of the Government Code, to read:

CHAPTER 20. GOVERNMENTAL ACCESS TO FINANCIAL RECORDS

ARTICLE 1. DECLARATION OF POLICY

7460. This chapter shall be known as the "California Right to Financial Privacy Act."

7461. The Legislature finds and declares as follows:

(a) Procedures and policies governing the relationship between financial institutions and government agencies have in some cases developed without due regard to citizens' constitutional rights.

(b) The California Supreme Court has recognized that there is a right to privacy under Section 13 of Article I of the California Constitution with respect to financial records held by a financial institution.

(c) The confidential relationships between financial institutions and their customers are built on trust and must be preserved and protected.

(d) The purpose of this chapter is to protect the confidential relationship between financial institutions and their customers and the constitutional rights of citizens inherent to that relationship.

ARTICLE 2. DEFINITIONS

7465. For the purposes of this chapter:

(a) The term "financial institution" includes state and national banks, state and federal savings and loan associations, trust companies, industrial loan companies, and state and federal credit unions.

(b) The term "financial records" means any original or any copy of any record or document held by a financial institution pertaining to a customer of the financial institution.

(c) The term "person" means an individual, partnership, corporation, association, trust, or any other legal entity organized under the laws of this state.

(d) The term "customer" means any person who has transacted business with or has used the services of a financial institution or for whom a financial institution has acted as a fiduciary.

(e) The term "state agency" means every state office, officer, department, division, bureau, board, and commission or other state agency.

(f) The term "local agency" includes a county; city, whether general law or chartered; city and county; school district; municipal corporation; district; political subdivision; or any board, commission or agency thereof; or other local public agency.

(g) The term "supervisory agency" means any of the following:

(1) The State Banking Department.

(2) The Department of Savings and Loans.

(3) The Department of Corporations.

(4) The State Controller.

(5) The Franchise Tax Board.

(6) The State Board of Equalization.

(h) The term "investigation" includes, but is not limited to, any inquiry by a peace officer, sheriff, or district attorney, or any inquiry made for the purpose of determining whether there has been a violation of any law enforceable by imprisonment, fine, or monetary liability.

ARTICLE 3. CONFIDENTIALITY OF, AND ACCESS TO, FINANCIAL RECORDS

7470. (a) Except as provided in Section 7480, no officer, employee, or agent of a state or local agency or department thereof, in connection with a civil or criminal investigation of a customer, whether or not such investigation is being conducted pursuant to formal judicial or administrative proceedings, may request or receive copies of, or the information contained in, the financial records of any customer from a financial institution unless the financial records are described with particularity and are consistent with the scope and requirements of the investigation giving rise to such request and:

(1) Such customer has authorized disclosure to such officer, employee or agent of such state or local agency or department thereof in accordance with Section 7473; or

(2) Such financial records are disclosed in response to an administrative subpoena or summons which meets the requirements of Section 7474; or

(3) Such financial records are disclosed in response to a search warrant which meets the requirements of Section 7475; or

(4) Such financial records are disclosed in response to a judicial subpoena or subpoena duces tecum which meets the requirements of Section 7476.

(b) In any proceeding relating to such subpoenas, summons, or search warrants, the customer shall have the same rights as if the records were in his possession.

(c) Nothing in this section or in Sections 7473, 7474, 7475, and 7476 shall require a financial institution to inquire or determine that those seeking disclosure have duly complied with the requirements set forth therein, provided only that the customer authorization, administrative subpoena or summons, search warrant, or judicial subpoena or order served on or delivered to a financial institution pursuant to such sections shows compliance on its face.

(d) The financial institution shall maintain for a period of five years a record

of all examinations or disclosures of the financial records of a customer including the identity and purpose of the person examining the financial records, the state or local agency or department thereof which he represents, and, where applicable, a copy of the customer authorization, subpoena, summons or search warrant providing for such examination or disclosure or a copy of the certified crime report received pursuant to subdivision (b) of Section 7480. Any record maintained pursuant to this subdivision shall be available at the office or branch where the customer's account is located during normal business hours for review by the customer upon request. A copy of such record shall be furnished to the customer upon request and payment of the reasonable cost thereof.

7471. (a) Except in accordance with requirements of Section 7473, 7474, 7475, or 7476, no financial institution, or any director, officer, employee, or agent of a financial institution, may provide or authorize another to provide to an officer, employee, or agent of a state or local agency or department thereof, any financial records, copies thereof, or the information contained therein, if the director, officer, employee or agent of the financial institution knows or has reasonable cause to believe that such financial records or information are being requested in connection with a civil or criminal investigation of the customer, whether or not such investigation is being conducted pursuant to formal judicial or administrative proceedings.

(b) This section is not intended to prohibit disclosure of the financial records of a customer or the information contained therein incidental to a transaction in the normal course of business of such financial institution if the director, officer, employee or agent thereof making or authorizing the disclosure has no reasonable cause to believe that the financial records or the information contained in the financial records so disclosed will be used by a state or local agency or department thereof in connection with an investigation of the customer, whether or not such investigation is being conducted pursuant to formal judicial or administrative proceedings.

(c) This section shall not preclude a financial institution, in its discretion, from initiating contact with, and thereafter communicating with and disclosing customer financial records to, appropriate state or local agencies concerning suspected violation of any law.

(d) A financial institution which refuses to disclose the financial records of a customer, copies thereof or the information contained therein, in reliance in good faith upon the prohibitions of subdivision (a) shall not be liable to its customer, to a state or local agency, or to any other person for any loss or damage caused in whole or in part by such refusal.

7472. Copies of financial records or the information contained therein, including information supplied pursuant to subdivision (b) of Section 7480, which are obtained by any state agency, local agency or supervisory agency may not be:

(a) Used or retained in any form for any purpose other than the specific statutory purpose for which the information was originally obtained; or

(b) Provided to any other governmental department or agency or other person except where authorized by state law. If in the course of an investigation conducted pursuant to the provisions of this chapter, an officer, employee, or agent of a state

or local agency or department thereof, discovers financial records indicating a possible violation of law which such agency is without statutory authority to investigate or prosecute, the information in such financial records may, in the discretion of the agency and unless otherwise precluded by law, be provided to the district attorney of the county in which such financial records were examined or to the Attorney General.

7473. (a) A customer may authorize disclosure under paragraph (1) of subdivision (a) of Section 7470 if those seeking disclosure furnish to the financial institution a signed and dated statement by which the customer:

(1) Authorizes such disclosure for a period to be set forth in the authorization statement;

(2) Specifies the name of the agency or department to which disclosure is authorized and, if applicable, the statutory purpose for which the information is to be obtained; and

(3) Identifies the financial records which are authorized to be disclosed.

(b) No such authorization shall be required as a condition of doing business with such financial institution.

(c) Any officer, employee or agent of a state or local agency seeking customer authorization for disclosure of customer financial records shall notify the customer that the customer has the right at any time to revoke such authorization, except where such authorization is required by statute.

(d) An agency or department examining the financial records of a customer pursuant to this section shall notify the customer in writing within 30 days of such examination. Such notice shall specify the financial records which were examined and the reason for such examination.

7474. (a) An officer, employee, or agent of a state or local agency or department thereof, may obtain financial records under paragraph (2) of subdivision (a) of Section 7470 pursuant to an administrative subpoena or summons otherwise authorized by law and served upon the financial institution only if:

(1) The person issuing such administrative summons or subpoena has served a copy of the subpoena or summons on the customer pursuant to Chapter 4 (commencing with Section 413.10) of Title 5 of Part 2 of the Code of Civil Procedure; and

(2) The subpoena or summons includes the name of the agency or department in whose name the subpoena or summons is issued and the statutory purpose for which the information is to be obtained; and

(3) The customer has not moved to quash such subpoena or summons within 10 days of service.

(b) Nothing in this chapter shall preclude a financial institution from notifying a customer of the receipt of an administrative summons or subpoena.

7475. An officer, employee, or agent of a state or local agency or department thereof, may obtain financial records under paragraph (3) of subdivision (a) of Section 7470 only if he obtains a search warrant pursuant to Chapter 3 (commencing with Section 1523) of Title 12 of Part 2 of the Penal Code. Examination

of financial records may occur as soon as the warrant is served on the financial institution.

7476. (a) An officer, employee, or agent of a state or local agency or department thereof, may obtain financial records under paragraph (4) of subdivision (a) of Section 7470 pursuant to a judicial subpoena or subpoena duces tecum only if:

(1) The subpoena or subpoena duces tecum is issued and served upon the financial institution and the customer in compliance with Chapter 2 (commencing with Section 1985) of Title 3 of Part 4 of the Code of Civil Procedure; and

(2) Ten days pass without notice to the financial institution that the customer has moved to quash the subpoena. If testimony is to be taken, or financial records produced, before a court, the 10-day period provided for in this subdivision may be shortened by the court issuing the subpoena or subpoena duces tecum upon a showing of reasonable cause. The court shall direct that all reasonable measures be taken to notify the customer within the time so shortened.

(b) (1) A grand jury, upon resolution adopted by a majority of its members, may obtain financial records pursuant to a judicial subpoena or subpoena duces tecum which upon a showing of probable cause, is personally signed and issued by a judge of the superior court in accordance with Section 939.2 of the Penal Code.

(2) Upon issuing such subpoena or subpoena duces tecum, the judge shall order the grand jury to notify the customer in writing within 30 days of such issuance; provided, however, that the judge may shorten the 30-day period, or upon a showing of good cause, may extend such period beyond 30 days, but not beyond the date on which such grand jury is to be discharged. The notice shall specify the financal records which were examined and the reason for such examination.

Article 4. Exceptions

7480. Nothing in this chapter prohibits any of the following:

(a) The dissemination of any financial information which is not identified with, or identifiable as being derived from, the financial records of a particular customer.

(b) When any police or sheriff's department or district attorney in this state certifies to a bank in writing that a crime report has been filed which involves the alleged fraudulent use of drafts, checks or other orders drawn upon any bank in this state, such police or sheriff's department or district attorney may request a bank to furnish, and a bank shall supply, a statement setting forth the following information with respect to a customer account specified by the police or sheriff's department or district attorney for a period 30 days prior to and up to 30 days following the date of occurrence of the alleged illegal act involving the account:

(i) The number of items dishonored;

(ii) The number of items paid which created overdrafts;

(iii) The dollar volume of such dishonored items and items paid which created

overdrafts and a statement explaining any credit arrangement between the bank and customer to pay overdrafts;

(iv) The dates and amounts of deposits and debits and the account balance on such dates;

(v) A copy of the signature appearing on a customer's signature card;

(vi) Date account opened and, if applicable, date account closed.

(c) Subject to the limitations in Section 7472, the examination by, or disclosure to, any supervisory agency of financial records which relate solely to the exercise of its supervisory function. The scope of an agency's supervisory function shall be determined by reference to statutes which grant authority to examine, audit, or require reports of financial records or financial institutions as follows:

(1) With respect to the Superintendent of Banks by reference to Division 1 (commencing with Section 99) of the Financial Code.

(2) With respect to the Department of Savings and Loans by reference to Division 2 (commencing with Section 5000) of the Financial Code.

(3) With respect to the Corporations Commissioner by reference to Division 5 (commencing with Section 14000) and Division 7 (commencing with Section 18000) of the Financial Code.

(4) With respect to the State Controller by reference to Title 10 (commencing with Section 1300) of Part 3 of the Code of Civil Procedure.

(5) With respect to the Franchise Tax Board and the Board of Equalization by reference to the Revenue and Taxation Code relating to the enforcement and administration of tax laws.

Article 5. Penalties and Remedies

7485. (a) Any person who willfully or knowingly participates in a violation of this chapter is guilty of a misdemeanor, and upon conviction shall be imprisoned for not more than one year, or fined not more than five thousand dollars ($5,000), or both.

(b) Any person who induces or attempts to induce a violation of this chapter is guilty of a misdemeanor and upon conviction shall be imprisoned for not more than one year, or fined not more than five thousand dollars ($5,000), or both.

7486. In any successful action to enforce liability for a violation of the provisions of this chapter, the customer may recover the cost of the action together with reasonable attorney's fees as determined by the court.

7487. In addition to any other remedy contained in this chapter or otherwise available, injunctive relief shall be available to any customer aggrieved by a violation, or threatened violation, of this chapter in the same manner as such injunctive relief would be available if the financial records concerning the customer accounts were in his possession. In any successful action by the customer, costs together with reasonable attorney's fees as determined by the court may be recovered.

7488. An action to enforce any provision of this chapter must be commenced within three years after the date on which the violation occurred.

Article 6. Miscellaneous

7490. Except as provided in Section 7473, no waiver by a customer of any right hereunder shall be valid, whether oral or written, and whether with or without consideration.

7491. Should any other law grant or appear to grant power or authority to any person to violate the provisions of this chapter, the provisions of this chapter shall supersede and pro tanto override and annul such law, except those statutes hereinafter enacted which specifically refer to this chapter.

7492. If any provision of this chapter or the application thereof to any person or circumstance is held invalid for any reason, such invalidity shall not affect any other provisions or applications of this chapter which can be effected, without the invalid provision or application, and to this end the provisions of this chapter are severable.

SECTION 5. Section 12537 of the Government Code is amended to read:

12537. The Attorney General shall maintain a register of health care service plans. On or before March 31 of the calendar year following the effective date of this article and annually thereafter, each health care service plan shall register with the Attorney General by submitting the name, organizational form and principal place of business of the plan and the following:

(a) A form of each standard membership contract which the plan proposes to issue, including standard forms in use on the date of submission.

(b) Copies of all advertising which the plan proposes to use.

(c) An authorization for disclosure to the Attorney General of financial records of the health care service plan pursuant to Section 7473 of the Government Code.

(d) Such other pertinent and relevant information as the Attorney General may reasonably require for the proper administration of this article; provided, however, that

(1) Nothing in this article shall affect or modify the physician-patient relationship prescribed in Section 1881 of the Code of Civil Procedure; and

(2) All information furnished under this paragraph (d) shall be kept confidential by the Attorney General, except to the extent that it may be produced in any judicial or administrative proceeding and may be admissible in evidence therein.

SECTION 6. Section 12586 of the Government Code is amended to read:

12586. (a) Except as otherwise provided and except corporate trustees which are subject to the jurisdiction of the Superintendent of Banks of the State of California or to the Comptroller of Currency of the United States, every charitable corporation and trustee subject to this article shall, in addition to filing copies of the instruments previously required, file with the Attorney General: (i) periodic written reports, under oath, setting forth information as to the nature of the assets held for charitable purposes and the administration thereof by the corporation or trustee, in accordance with rules and regulations of the Attorney General; (ii) an authorization for disclosure to the Attorney General of financial records of the charitable corporations pursuant to Section 7473 of the Government Code.

(b) The Attorney General shall make rules and regulations as to the time for filing reports, the contents thereof, and the manner of executing and filing them. He may classify trusts and other relationships concerning property held for a charitable purpose as to purpose, nature of assets, duration of the trust or other relationship, amount of assets, amounts to be devoted to charitable purposes, nature of trustee, or otherwise, and may establish different rules for the different classes as to time and nature of the reports required to the ends (1) that he shall receive reasonably current, periodic reports as to all charitable trusts or other relationships of a similar nature, which will enable him to ascertain whether they are being properly administered, and (2) that periodic reports shall not unreasonably add to the expense of the administration of charitable trusts and similar relationships. The Attorney General may suspend the filing of reports as to a particular charitable trust or relationship for a reasonable, specifically designated time upon written application of the trustee filed with the Attorney General and after the Attorney General has filed in the register of charitable trusts a written statement that the interests of the beneficiaries will not be perjudiced thereby and that periodic reports are not required for proper supervision by his office.

(c) A copy of an account filed by the trustee in any court having jurisdiction of the trust or other relationship, if the account substantially complies with the rules and regulations of the Attorney General, may be filed as a report required by this section.

(d) The first report for a trust or similar relationship hereafter established, unless the filing thereof is suspended as herein provided, shall be filed not later than four (4) months and fifteen (15) days following the close of the first calendar or fiscal year in which any part of the income or principal is authorized or required to be applied to a charitable purpose. If any part of the income or principal of a trust previously established is authorized or required to be applied to a charitable purpose at the time this article takes effect, the first report shall be filed at the close of the calendar or fiscal year in which it was registered with the Attorney General or not later than four (4) months and fifteen (15) days following the close of such calendar or fiscal period.

SECTION 7. Section 904 is added to the Insurance Code, to read:

904. In addition to the annual statement required to be filed pursuant to Section 900, each admitted insurer shall file an authorization for disclosure to the commissioner of financial records pertaining to such funds pursuant to Section 7473 of the Government Code, to be effective until the next such annual filing.

SECTION 8. Section 1703 is added to the Insurance Code, to read:

1703. Every applicant for an original or a renewal license to act as an insurance agent, broker or solicitor, life agent, life analyst, surplus line broker, special lines surplus line broker, motor club agent, or bail agent or solicitor shall, as part of the application, endorse an authorization for disclosure to the commissioner of financial records of any fiduciary funds as defined in Section 1733, pursuant to Section 7473 of the Government Code.

SECTION 9. Section 11703 of the Vehicle Code is amended to read:

11703. The department may refuse to issue a license and special plates to a manufacturer, manufacturer branch, distributor, distributor branch, transporter, or dealer, when it determines that:

(a) The applicant was previously the holder of a license and special plates issued under this chapter, which license and special plates were revoked for cause and never reissued by the department, or which license was suspended for cause and the terms of suspension have not been fulfilled.

(b) The applicant was previously a limited or general partner, stockholder, director, or officer of a partnership or corporation whose license and special plates issued under the authority of this chapter were revoked for cause and never reissued or were suspended for cause and the terms of suspension have not been terminated.

(c) If the applicant is a partnership or corporation, that one or more of the limited or general partners, stockholders, directors or offices was previously the holder or a limited or general partner, stockholder, director or officer of a partnership or corporation whose license and special plates issued under the authority of this chapter were revoked for cause and never reissued or were suspended for cause and the terms of suspension have not been terminated, or that by reason of the facts and circumstances touching the organization, control, and management of the partnership or corporation business the policy of such business will be directed, controlled, or managed by individuals who, by reason of their conviction of violations of the provisions of this code, would be ineligible for a license and that by licensing such corporation or partnership the purposes of this code would likely be defeated.

(d) The applicant, or one of the limited or general partners, if the applicant be a partnership, or one or more of the officers or directors of the corporation, if the corporation be the applicant, or one or more of the stockholders if the policy of such business will be directed, controlled, or managed by such stockholder or stockholders, has ever been convicted of a felony or a crime involving moral turpitude. A conviction after a plea of nolo contendere is deemed to be a conviction within the meaning of this section.

(e) The information contained in the application is incorrect.

(f) The decision of the department to cancel, suspend or revoke a license has been entered, and this applicant was the licensee, a copartner, or an officer, director or stockholder of such licensee.

(g) An applicant for a dealer's license has failed to effectively endorse an authorization for disclosure of an account or accounts relating to the operation of the dealership as provided for in Section 7473 of the Government Code.

SECTION 10. No appropriation is made by this act, nor is any obligation created thereby under Section 2231 of the Revenue and Taxation Code, for the

reimbursement of any local agency for any costs that may be incurred by it in carrying on any program or performing any service required to be carried on or peformed by it by this act because the Legislature recognizes that during any legislative session a variety of changes to laws relating to crimes and infractions may be enacted that serve to cause both increased and decreased costs to local governmental entities which, in the aggregate, do not result in significant identifiable cost changes.

Assembly Concurrent Resolution No. 192

STATE OF NEW JERSEY

Introduced July 22, 1974

By Assemblymen BURSTEIN, HYNES, MARTIN and BAER

REFERRED TO COMMITTEE ON JUDICIARY, LAW, PUBLIC SAFETY AND DEFENSE

A Concurrent Resolution creating a commission to study the matter of invasion of personal privacy.

Whereas, The right of privacy of the individual is among the most sacred and inalienable rights of man in society, and is a principle implicit in the concept of a free and just society; and

Whereas, The privacy of the individual has become increasingly susceptible to encroachment in modern society because of sophisticated and novel innovations and methods in numerous fields of science and technology rendering existing law inadequate in some instances to protect said privacy; and

Whereas, Many of the worst invasions of privacy in New Jersey come from insensitive and intrusive actions by local businesses and State and local government agencies, such as, commercial reporting agencies, police arrest records, and public school questionnaires; and

Whereas, The privacy of the individual must be protected from the misuse of records and computer data banks; and

Whereas, It is the duty of the legislative branch of government to inquire into and provide remedies for any inequities that may exist; now, therefore

Be it resolved *by the General Assembly of the State of New Jersey (the Senate concurring):*

1. There is hereby created a commission to consist of eight members, four to be appointed by the President of the Senate, two to be Senators and two to be citizens from the State at large, and four to be appointed by the Speaker of the General Assembly, two to be members of the General Assembly and two to be citizens from the State at large. No more than one of each group of two shall be of the same political party. The members shall serve without compensation. Vacancies in the membership of the commission shall be filled in the same manner as the original appointments were made.

2. The commission shall organize as soon as may be after the appointment of

its members and shall select a chairman from among its members and a secretary who need not be a member of the commission.

3. It shall be the duty of said commission to study the methods by which the right of privacy may be invaded and the extent thereof, to investigate such invasions of privacy, to evaluate the justifications of such invasions, to determine the necessity for corrective action, and to make recommendations for protective measures and legislation as it deems desirable and appropriate.

4. The commission shall be entitled to call to its assistance and avail itself of the services of such employees of any State, county or municipal department, board, bureau, commission or agency as it may require and as may be available to it for said purpose, and to employ counsel and such stenographic and clerical assistants and incur such traveling and other miscellaneous expenses as it may deem necessary, in order to perform its duties, and as may be within the limits of funds appopriated or otherwise made available to it for said purposes.

5. The commission may meet and hold hearings at such place or places as it shall designate during the sessions or recesses of the Legislature and shall report its findings and recommendations to the Legislature, accompany the same with any legislative bills which it may desire to recommend for adoption by the Legislature.

STATEMENT

The purpose of this resolution is to create a commission which shall study and make recommendations concerning the invasion of personal privacy and recommend protective measures for the increasing encroachment in our society upon the privacy of the individual.

STATE OF OKLAHOMA

An Act

ENROLLED HOUSE BILL NO. 1652

BY: MONKS and WILLIAMS of the House and PIERCE and FUNSTON of the Senate

AN ACT RELATING TO STATE GOVERNMENT; PROHIBITING THE USE OF SOCIAL SECURITY NUMBERS BY STATE AGENCIES, BOARDS, COMMISSIONS OR OTHER SUBDIVISIONS OF STATE GOVERNMENT; PROVIDING CERTAIN EXEMPTIONS; PROHIBITING DISCLOSURE OF INFORMATION INDEXED BY SOCIAL SECURITY NUMBERS; AND PROHIBITING THE REQUIRING OF DISCLOSURE OF ONE'S SOCIAL SECURITY NUMBER FOR THE ISSUANCE OF LICENSES BY THE DEPARTMENT OF PUBLIC SAFETY.

Be it enacted by the people of the State of Oklahoma:

SECTION 1. No state agency, board, commission or other unit or subdivision of state government shall request or require that any person reveal his social security number in order to obtain services or assistance, nor shall any state agency, board, commission or other unit or subdivision of state government use, for any purpose, numbers which correspond to the social security number of any person. Provided that any state agency, board, commission, unit or subdivision of state government using social security numbers for a particular purpose prior to January 1, 1974, may continue to use and require social security numbers for that purpose only and provided, further, that the provisions of this act shall not be construed to prohibit the use or requirement of disclosure of one's social security number if the use of the number is related to the Social Security Administration or benefits thereunder.

SECTION 2. The Oklahoma Department of Public Safety shall not deny or refuse to issue any license because of the failure of any person to disclose his social security number upon application for or renewal of such license and the Department shall not indicate in any manner that the furnishing of such number is mandatory or required for the issuance of such license or any renewal thereof.

SECTION 3. No state agency, board, commission or other unit or subdivision of state government may furnish any information indexed by social security number unless required by law or specifically authorized to do so by the holder of said social security number. Provided that this section shall not apply to a report produced by a state agency of monetary payments made to any state official or employee from State Treasury funds or accounts.

Signed into law 3 May 1974.

THE PRIVACY ACT OF 1974

PUBLIC LAW 93-579
93RD CONGRESS, S. 3418
December 31, 1974

AN ACT

To amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records, to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, to establish a Privacy Protection Study Commission, and for other purposes.

Privacy Act of 1974.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Privacy Act of 1974".

Congressional findings.

SEC. 2. (a) The Congress finds that—

(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

(2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;

(3) the opportunities for an individual to secure employment insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

Statement of purpose.

(b) The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to—

(1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies;

(2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;

(3) permit an individual to gain access to information pertaining to him in

Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;

(4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;

(5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

(6) be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under this Act.

SEC. 3. Title 5, United States Code, is amended by adding after section 552 the following new section:

"§ 552a. Records maintained on individuals

"(a) DEFINITIONS.—For purposes of this section—

"(1) the term 'agency' means agency as defined in section 552 (e) of this title;

"(2) the term 'individual means a citizens of the United States or an alien lawfully admitted for permanent residence;

"(3) the term 'maintain' includes maintain, collect, use, or disseminate;

"(4) the term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;

"(5) the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual;

"(6) the term 'statistical record' means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13; and

"(7) the term 'routine use' means, with respect to the disclosure of a record, for a purpose which is compatible with the purpose for which it was collected.

"(b) CONDITIONS OF DISCLOSURE.—No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—

"(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

"(2) required under section 552 of this title;

"(3) for a routine use as defined in subsection (a) (7) of this section and described under subsection (e) (4) (D) of this section;

"(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;

"(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

"(6) to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government or for evaluation of the Administration of General Services or his designee to determine whether the record has such value;

"(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

"(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;

"(9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;

"(10) to the Comptroller General, or any of his authorized representatives, in the course of performance of the duties of the General Accounting Office; or

"(11) pursuant to the order of a court of competent jurisdiction.

"(c) ACCOUNTING OF CERTAIN DISCLOSURES.—Each agency, with respect to each system of records under its control, shall—

"(1) except for disclosures made under subsections (b) (1) or (b) (2) of this section, keep an accurate accounting of—

"(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

"(B) the name and address of the person or agency to whom disclosure is made;

"(2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;

"(3) except for disclosures made under subsection (b) (7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

"(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

"(d) ACCESS TO RECORDS.—Each agency that maintains a system of records shall—

Personal review.

"(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence;

Amendment request.

"(2) permit the individual to request amendment of a record pertaining to him and—

"(A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and

"(B) promptly, either—

"(i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

"(ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official;

Review.

"(3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review, and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g) (1) (A) of this section;

Notation of dispute.

"(4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of the subsection, clearly note any portion of the record which is

disputed and provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and

"(5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

"(e) AGENCY REQUIREMENTS.—Each agency that maintains a system of records shall—

"(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;

"(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;

"(3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual—

"(A) the authority (whether granted by statute, or by executive statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;

"(B) the principal purposes for which the information is intended to be used;

"(C) the routine uses which may be made of the information, as published pursuant to paragraph (4) (D) of this subsection; and

"(D) the effects on him, if any, of not providing all or any part of the requested information;

Publication in Federal Register.

"(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register at least annually a notice of the existence and character of the system of records, which notice shall include—

"(A) the name and location of the system;

"(B) the categories of individuals on whom records are maintained in the system;

"(C) the categories of records maintained in the system;

"(D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;

"(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

"(F) the title and business address of the agency official who is responsible for the system of records;

"(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;

"(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and

"(I) the categories of sources of records in the system;

"(5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;

"(6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b) (2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;

"(7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;

"(8) make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record;

Rules of Conduct

"(9) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance;

Confidentiality of Records

"(10) establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained; and

Publication in Federal Register.

"(11) at least 30 days prior to publication of information under paragraph (4) (D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency.

"(f) AGENCY RULES.—In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall—

"(1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;

"(2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;

"(3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;

"(4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section: and

Fees.

"(5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

Publication in Federal Register.

The Office of the Federal Register shall annually compile and publish the rules promulgated under this subsection and agency notices published under subsection (e) (4) of this section in a form available to the public at low cost.

"(g) (1) CIVIL REMEDIES.—Whenever any agency

"(A) makes a determination under subsection (d) (3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;

"(B) refuses to comply with an individual request under subsection (d) (1) of this section;

"(C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or

"(D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual,

Jurisdiction.

the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

Amendment of record.

"(2) (A) In any suit brought under the provisions of subsection (g) (1) (A) of this section, the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct. In such a case the court shall determine the matter de novo.

"(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

Injunction.

"(3) (A) In any suit brought under the provisions of subsection (g) (1) (B) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and

may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the agency to sustain its action.

"(B) The court may asses against the United States reasonable attorney fees and other litigation cost reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

Damages.

"(4) In any suit brought under the provisions of subsection (g) (1) (C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of—

"(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000; and

"(B) the costs of the action together with reasonable attorney fees as determined by the court.

"(5) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to the effective date of this section.

"(h) RIGHTS OF LEGAL GUARDIANS.—For the purposes of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

"(i) (1) CRIMINAL PENALTIES.—Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

"(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e) (4) of this section shall be guilty of a misdemeanor and fined not more than $5,000.

"(3) Any person who knowingly and willfully requests or obtains any record

concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

"(j) GENERAL EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553 (b) (1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c) (1) and (2), (e) (4) (A) through (F), (e) (6), (7), (9), (10) (11), and (i) if the system of records is—

"(1) maintained by the Central Intelligence Agency; or

"(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553 (c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

"(K) SPECIFIC EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553 (b) (1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c) (3), (d), (e) (1), (e) (4) (G), (H), and (I) and (f) of this section if the system of records is—

"(1) subject to the provisions of section 552 (b) (1) of this title;

"(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j) (2) of this section: *Provided, however,* That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

"(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18;

"(4) required by statute to be maintained and used solely as statistical records;

"(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

"(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or

"(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553 (c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

"(1) (1) ARCHIVAL RECORDS.—Each agency record which is accepted by the Administrator of General Services for storage, processing, and servicing in accordance with section 3103 of title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Administrator of General Services shall not disclose the record except to the agency which maintains the record, or under rules established by that agency which are not inconsistent with the provisions of this section.

"(2) Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section, except that a statement generally describing such records (modeled after the requirements relating to records subject to subsections (e) (4) (A) through (G) of this section) shall be published in the Federal Register.

Publication in Federal Register.

"(3) Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of

this section, be considered to be maintained by the National Archives and shall be exempt from the requirements of this section except subsections (e) (4) (A) through (G) and (e) (9) of this section.

"(m) GOVERNMENT CONTRACTORS.—When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.

"(n) MAILING LISTS.—An individual's name and address may not be sold or rented by an agency unless such action is specifically authorized by law. This provision shall not be construed to require the withholding of names and addresses otherwise permitted to be made public.

Notice to Congress and OMB.

"(o) REPORT ON NEW SYSTEMS.—Each agency shall provide adequate advance notice to Congress and the Office of Management and Budget of any proposal to establish or alter any system of records in order to permit an evaluation of the probable or potential effect of such proposal on the privacy and other personal or property rights of individuals or the disclosure of information relating to such individuals, and its effect on the preservation of the constitutional principles of federalism and separation of powers.

Report to Speaker of the House and President of the Senate.

"(p) ANNUAL REPORT.—The President shall submit to the Speaker of the House and the President of the Senate, by June 30 of each calendar year, a consolidated report, separately listing for each Federal agency the number of records contained in any system of records which were exempted from the application of this section under the provisions of subsections (j) and (k) of this section during the preceding calendar year, and the reasons for the exemptions, and such other information as indicates efforts to administer fully this section.

(q) EFFECT OF OTHER LAWS.—No agency shall rely on any examination contained in section 552 of this title to withhold from an individual any record which is otherwise accessible to such individual under the provisions of this section."

SEC. 4. The chapter analysis of chapter 5 of title 5, United States Code, is amended by inserting:

"552a. Records about individuals."

immediately below:

"552. Public information; agency rules, opinions, orders, and proceedings".

Privacy Protection Study Commission. Establishment. Membership.

SEC. 5. (a) (1) There is established a Privacy Protection Study Commission (hereinafter referred to as the "Commission") which shall be composed of seven members as follows:

(A) three appointed by the President of the United States,

(B) two appointed by the President of the Senate, and

(C) two appointed by the Speaker of the House of Representatives.

Members of the Commission shall be chosen from among persons who, by reason

of their knowledge and expertise in any of the following areas—civil rights and liberties, law, social sciences, computer technology, business, records management, and State and local government—are well qualified for service on the Commission.

(2) The members of the Commission shall elect a Chairman from among themselves.

Vacancies.

(3) Any vacancy in the membership of the Commission, as long as there are four members in office, shall not impair the power of the Commission but shall be filled in the same manner in which the original appointment was made.

(4) A quorum of the Commission shall consist of a majority of the members, except that the Commission may establish a lower number as a quorum for the purpose of taking testimony. The Commission is authorized to establish such committees and delegate such authority to them as may be necessary to carry out its functions. Each member of the Commission, including the Chairman, shall have equal responsibility and authority in all decisions and actions of the Commission, shall have full access to all information necessary to the performance of their functions, and shall have one vote. Action of the Commission shall be determined by a majority vote of the members present. The Chairman (or a member designated by the Chairman to be acting Chairman) shall be the official spokesman of the Commission in its relations with the Congress, Government agencies, other persons, and the public, and, on behalf of the Commission, shall see to the faithful execution of the administrative policies and decisions of the Commission, and shall report thereon to the Commission from time to time or as the Commission may direct.

Budget requests.

(5) (A) Whenever the Commission submit any budget estimate or request to the President or the Office of Management and Budget, it shall concurrently transmit a copy of that request to Congress.

Legislative recommendations.

(B) Whenever the Commission submits any legislative recommendations, or testimony, or comments on legislation to the President or Office of Management and Budget, it shall concurrently transmit a copy thereof to the Congress. No officer or agency of the United States shall have any authority to require the Commission to submit its legislative recommendations, or testimony, or comments on legislation, to any officer or agency of the United States for approval, comments, or review, prior to the submission of such recommendations, testimony, or comments to the Congress.

(b) The Commission shall—

Study.

(1) make a study of the data banks, automated data processing programs, and information systems of governmental, regional, and private organizations, in order to determine the standards and procedures in force for the protection of personal information; and

(2) recommend to the President and the Congress the extent, if any, to which the requirements and principles of section 552a of title 5, United States Code, should be applied to the information practices of those organizations by legislation, administrative action, or voluntary adoption of such requirements and principles, and report on such other legislative recommendations as it may

determine to be necessary to protect the privacy of individuals while meeting the legitimate needs of government and society for information.

(c) (1) In the course of conducting the study required under subsection (b) (1) of this section, and in its reports thereon, the Commission may research, examine, and analyze—

(A) interstate transfer of information about individuals that is undertaken through manual files or by computer or other electronic or telecommunications means;

(B) data banks and information programs and systems the operation of which significantly or substantially affect the enjoyment of the privacy and other personal and property rights of individuals;

(C) the use of social security numbers, license plate numbers, universal identifiers, and other symbols to identify individuals in data banks and to gain access to, integrate, or centralize information systems and files; and

(D) the matching and analysis of statistical data, such as Federal census data, with other sources of personal data, such as automobile registries and telephone directories, in order to reconstruct individual responses to statistical questionnaires for commercial or other purposes, in a way which results in a violation of the implied or explicitly recognized confidentiality of such information.

(2) (A) The Commission may include in its examination personal information activities in the following areas: medical; insurance; education; employment and personnel; credit, banking and financial institutions; credit bureaus; the commercial reporting industry; cable television and other telecommunications media; travel, hotel and entertainment reservations; and electronic check processing.

(B) The Commission shall include in its examination a study of—

(i) whether a person engaged in interstate commerce who maintains a mailing list should be required to remove an individual's name and address from such list upon request of that individual;

(ii) whether the Internal Revenue Service should be prohibited from transfering individually indentifiable data to other agencies and to agencies of State governments;

(iii) whether the Federal Government should be liable for general damages incurred by an individual as the result of a willful or intentional violation of the provisions of sections 552a (g) (1) (C) or (D) of title 5, United States Code; and

(iv) whether and how the standards for security and confidentiality of records required under section 552a (c) (10) of such title should be applied when a record is disclosed to a person other than an agency.

Religious organizations, exception.

(C) The Commission may study such other personal information activities necessary to carry out the congressional policy embodied in this Act, except that the Commission shall not investigate information systems maintained by religious organizations.

Guidelines for study.

(3) In conducting such study, the Commission shall—

(A) determine what laws, Executive orders, regulations, directives, and judicial decisions govern the activities under study and the extent to which they are consistent with the rights of privacy, due process of law, and other guarantees in the Constitution;

(B) determine to what extent governmental and private information systems affect Federal-State relations or the principle of separation of powers;

(C) examine the standards and criteria governing programs, policies, and practices relating to the collection, soliciting, processing, use, access, integration, dissemination, and transmission of personal information; and

(D) to the maximum extent practicable, collect and utilize findings, reports, studies, hearing transcripts, and recommendations of governmental, legislative and private bodies, institutions, organizations, and individuals which pertain to the problems under study by the Commission.

(d) In addition to its other functions the Commission may—

(1) request assistance of the heads of appropriate departments, agencies, and instrumentalities of the Federal Government, of State and local governments, and other persons in carrying out its functions under this Act;

(2) upon request, assist Federal agencies in complying with the requirements of section 552a of title 5, United States Code;

(3) determine what specific categories of information, the collection of which would violate an individual's right of privacy, should be prohibited by statute from collection by Federal agencies; and

(4) upon request, prepare model legislation for use by State and local governments in establishing procedures for handling, maintaining, and disseminating personal information at the State and local level and provide such technical assistance to State and local governments as they may require in the preparation and implementation of such legislation.

(e) (1) The Commission may, in carrying out its functions under this section, conduct such inspections, sit and act at such times and places, hold such hearings, take such testimony, require by subpena the attendance of such witnesses and the production of such books, records, papers, correspondence, and documents, administer such oaths, have such printing and binding done, and make such expenditures as the Commission deems advisable. A subpena shall be issued only upon an affirmative vote of a majority of all members of the Commission. Subpenas shall be issued under the signature of the Chairman or any member of the Commission designated by the Chairman and shall be served by any person designated by the Chairman or any such member. Any member of the Commission may administer oaths or affirmations to witnesses appearing before the Commission.

Reports, transmittal to Commission

(2) (A) Each department, agency, and instrumentality of the executive branch of the Government is authorized to furnish to the Commission, upon request made by the Chairman, such information, data, reports and such other assistance as the Commission deems necessary to carry out its functions under this section. When-

ever the head of any such department, agency, or instrumentality submits a report pursuant to section 552a (o) of title 5, United States Code, a copy of such report shall be transmitted to the Commission.

(B) In carrying out its functions and exercising its powers under this section, the Commission may accept for many such department, agency, independent instrumentality, or other person any individually indentifiable data if such data is necessary to carry out such powers and functions. In any case in which the Commission accepts any such information, it shall assure that the information is used only for the purpose for which it is provided, and upon completion of that purpose such information shall be destroyed or returned to such department, agency, independent instrumentality, or person from which it is obtained, as appropriate.

(3) The Commission shall have the power to—

(A) appoint and fix the compensation of an executive director, and such additional staff personnel as may be necessary, without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and without regard to chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates, but at rates not in excess of the maximum rate for GS–18 of the General Schedule under section 5332 of such title; and

(B) procure temporary and intermittent services to the same extent as is authorized by section 3109 of title 5, United States Code.

The Commission may delegate any of its functions to such personnel of the Commission as the Commission may designate and may authorize such successive redelegations of such functions as it may deem desirable.

(4) The Commission is authorized—

Rules and regulations.

(A) to adopt, amend, and repeal rules and regulations governing the manner of its operations, organization, and personnel;

(B) to enter into contracts or other arrangements or modifications thereof, with any government, any department, agency, or independent instrumentality of the United States, or with any person, firm, association, or corporation, and such contracts or other arrangements, or modifications thereof, may be entered into without legal consideration, without performance or other bonds, and without regard to section 3709 of the Revised Statutes, as amended (41 U.S.C.5);

(C) to make advance, progress, and other payments which the Commission deems necessary under this Act without regard to the provisions of section 3648 of the Revised Statutes, as amended (31 U.S.C.529); and

(D) to take such other action as may be necessary to carry out its functions under this section.

Compensation.

(f) (1) Each [the] member of the Commission who is an officer or employee of the United States shall serve without additional compensation, but shall continue to receive the salary of his regular position when engaged in the performance of the duties vested in the Commission.

(2) A member of the Commission other than one to whom paragraph (1) applies shall receive per diem at the maximum daily rate for GS–18 of the General Schedule when engaged in the actual performance of the duties vested in the Commission.

Per diem.

(3) All members of the Commission shall be reimbursed for travel, subsistence, and other necessary expenses incurred by them in the performance of the duties vested in the Commission.

Travel expenses.

(g) The Commission shall, from time to time, and in an annual report, report to the President and the Congress on its activities in carrying out the provisions of this section. The Commission shall make a final report to the President and to the Congress on its findings pursuant to the study required to be made under subsection (b) (1) of this section not later than two years from the date on which all of the members of the Commission are appointed. The Commission shall cease to exist thirty days after the date on which final report is submitted to the President and the Congress.

Report to President and Congress.

(h) (1) Any member, officer, or employee of the Commission, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

Penalties.

(2) Any person who knowingly and willfully requests or obtains any record concerning an individual from the Commission under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

SEC. 6. The Office of Management and Budget shall—

(1) develop guidelines and regulations for the use of agencies in implementing the provisions of section 552a of title 5, United States Code, as added by section 3 of this Act; and

(2) provide continuing assistance to and oversight of the implementation of the provisions of such section by agencies.

SEC. 7. (a) (1) It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number.

(2) the provisions of paragraph (1) of this subsection shall not apply with respect to—

(A) any disclosure which is required by Federal statute, or

(B) the disclosure of a social security number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

(b) Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether

that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

Effective date.

SEC. 8. The provisions of this Act shall be effective on and after the date of enactment, except that the amendments made by sections 3 and 4 shall become effective 270 days following the day on which this Act is enacted.

Appropriation.

SEC. 9. There is authorized to be appropriated to carry out the provisions of section 5 of this Act for fiscal years 1975, 1976, and 1977 the sum of $1,500,000, except that not more than $750,000 may be expended during any such fiscal year.

Approved December 31, 1974.

LEGISLATIVE HISTORY:

HOUSE REPORT No. 93–1416 accompanying H.R. 16373 (Comm. on Government Operations.)

SENATE REPORT No. 93–1183 (Comm. on Government Operations).

CONGRESSIONAL RECORD, Vol. 120 (1974):

Nov. 21, considered and passed Senate.

Dec. 11, considered and passed House, amended, in lieu of H.R. 16373.

Dec. 17, Senate concurred in House amendment with amendments.

Dec. 18, House concurred in Senate amendments.

WEEKLY COMPILATION OF PRESIDENTIAL DOCUMENTS, Vol. 11, No. 1:

Jan. 1, Presidential statement.

A COMMENT ON THE PRIVACY ACT OF 1974

By Carole W. Parsons*

THE PRIVACY ACT has been a subject of discussion and controversy since its inception in 1974 hearings before the House Subcommittee on Foreign Operations and Government Information. It has been praised as a major step toward restoring citizen confidence in government, as a needed brake on the data-gathering appetite of Federal agencies, and as a welcome incentive to improve the efficiency of Federal agency record-keeping practices. It has been denounced as an obstacle to the exposure of elements in the society (including miscreant bureaucrats whose activities ought not to be shielded from public view, as a gratuitous constraint on the development of new record-keeping applications of computer and telecommunications technology, and as an administrative nightmare that promises to disrupt the normal operations of government and cause a permanent hemorrhage in the administrative budget of the Executive branch.

Despite these sharply contrasting expectations, however, both advocates and opponents of the Act have recognized from the beginning that its success or failure will depend in large measure on the spirit and skill with which it is administered.

When the Privacy Act took effect on September 27, 1975, the protection of personal privacy and the efficient management of government programs became inextricably entwined with administrative concerns. Line management — that is, agency heads and program managers — became directly responsible for assuring faithful and effective compliance with the Act's requirements. Agency practices that affect the collection, handling, and disclosure of information about individuals are now, by and large, a matter of public record. The individual citizen is in most cases guaranteed the right to see, challenge, and correct information in a record that an agency maintains about him for program purposes.

From now on agency proposals to establish or substantially alter a system of records about individuals will be scrutinized with a view to striking an acceptable balance between management needs for recorded personal information and the individual citizen's interest in limiting the content, character, and circulation of such information about him.

To understand this major shift in Federal policy on personal-data record keeping and to comprehend its various practical implications, one must bear in mind the intent of the Privacy Act. One objective, clearly, is to allay public anxiety about the possibility of illegal, unauthorized, and surreptitious disclosures and exchanges of personal information among Federal agencies themselves and between Federal agencies and other types of record-keeping organizations at other levels of government and in the private sector.

Another equally clear objective is to assure responsible, fair, safe, and cost-effective use of automated information processing technologies in the performance of personal data record-keeping functions in government. Still another — the one with the potential for the most far-reaching consequence of all — is to induce Federal agencies to behave in ways that reassure the individual citizen that the information he discloses about himself will indeed be used in a fair and judicious manner. As the now familiar HEW report on computers and privacy points out, it is characteristic of present day American society for an individual to be asked to

> 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 . . . .*

This situation, the report suggests, may be the principal source of public concern about the protection of personal privacy — far more important than the seemingly voracious organizational appetite for personal information — and it is the situation to which the Privacy Act is centrally addressed. By making the personal data record-keeping functions

* Carole W. Parsons, formerly Associate Executive Director of the Domestic Council Committee on the Right of Privacy, is Executive Director of the Privacy Protection Study Commission.

* *Records, Computers, and the Rights of Citizens*, see appendix V.

of government tangible — that is, open to public scrutiny — and by affording the individual an opportunity to affect those functions when he needs to do so on his own behalf, the Act, if administered in the proper spirit, should go far toward relieving the troubling sense of opacity and remoteness that has surrounded government record-keeping practices in the past.

REQUIREMENT OF THE ACT

The Office of Management and Budget has issued guidelines to Federal agencies on implementation of the Privacy Act's requirements. These guidelines, which are available to interested members of the public,* contain a detailed explanation of each of the Act's agreements. What follows here is only a brief summary of its principal features.

The first thing to be noted about the Act is that it applies exclusively to the handling of Federal records about individual citizens of the United States and aliens lawfully admitted for permanent residence. Moreover, it applies only to such records when they are maintained by an Executive branch agency in a system of records.

"Executive branch agency", as defined in the Act, means any executive department, Government corporation, Government-controlled corporation or other establishment in the executive branch of the Federal Government, including the Executive Office of the President or any independent regulatory agency, but specifically excluding any Congressional entity (such as the General Accounting Office) or any agency of the Judiciary. A "system of records" as defined in the Act, means

> a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

Within this scope of application, the Act requires each agency to do four basic things from which a range of other more specific requirements then flow logically:

> First, it requires the agency to assure that any personal information it maintains in a system is both germane and necessary to the performance of a function the agency is required to perform by statute or Executive order;
>
> Second, it requires the agency to publish in the *Federal Register* an annual notice that details such items as the name and location of each system the agency maintains, the types of records in the system, and the kinds of individuals to whom the records pertain, the policies and practices of the agency regarding storage, retrievability, retention, and disposal of the records, and the title and business address of the agency official responsible for the system;
>
> Third, it requires the agency to establish various types of procedures—including those that allow an individual to review and challenge a record about himself—so that when a record in one of the agency's systems is used to make a decision about an individual, it will be as accurate, complete, timely, and relevant as is necessary to assure that the record itself is not the cause of an unfair decision; and
>
> Fourth, it requires the agency to observe certain minimum restrictions on disclosure or dissemination including keeping an accounting of such.

Several points should be noted about these requirements.

First, the Act strongly reaffirms the principle that agency functions (at least to the extent they are supported by systematic record keeping about individuals) should be limited to those clearly authorized by statute or Executive order.

Second, the universality of the requirements to issue an annual public notice on each system of records an agency maintains cannot be overemphasized. No Federal agency system of records (as defined) is exempt. A guiding principle to which the public notice provision is directly responsive is that in a democratic society no government agency should maintain a record-keeping system on individuals without at least making the existence of the system a matter of public record.

Third, in the vast majority of cases the steps an agency takes to assure the accuracy, relevance, timeliness, and completeness of a record about an individual shall include procedures that give the individual an opportunity to confront the record in question. With certain exceptions an agency must give an individual access to a record that it maintains about him and permit him to challenge its content through a process established by the agency in accordance with the informal rule-making requirements (including general notice) of Section 553 of the Administrative Procedure Act — that is, notice of rule making and at least 30 days to receive and consider comment from interested members of the public.

Fourth, it is important to note that the "conditions of disclosure" section does not *require* an agency to make any of the disclosures the section authorizes, and in that sense should not be interpreted as contravening any existing, more stringent statutory prohibition on the disclosure of personal information. It is a set of minimum standards that operates in the context of other constraints on agency behavior, and one that in several instances gives agency heads and program managers the option of fashioning their own extremely tight disclosure policies. The "need-to-know" standard with respect to internal agency dissemination of a record, for example, can be drawn narrowly, and the decision whether or not to permit certain disclosures of records, even once they are established as "routine" disclosures, is to a large extent a discretionary matter for each agency.

Many other provisions must be considered in assessing the Act's likely practical effects. One provision, for example, narrows the circumstances under which an agency may record information about an individual's political and religious beliefs.

Several provisions stipulate or imply establishment of administrative and technical safeguards to assure that the Act's requirements will be consistently met. One feature of the Act that needs to be understood is the opportunity it provides to exempt systems of records from certain of its requirements. The Privacy Act places the responsibility for assuring faithful and effective compliance with its various requirements squarely on agency heads and program managers. Under the Act the decisions and actions of these officials are subject to court review. However, there is no interdepartmental review function or appeals board or other centralized arrangement for deciding when a program function cannot be carried out effectively if the record-keeping systems that serve it have to meet all of the Privacy Act's requirements. Some legitimate investigative activities, for example, would be totally frustrated if the individuals being investigated had immediate access to all the records being kept about them.

The solution to this dilemma is found in the provisions wherein an agency may seek an exemption from certain specified requirements for certain specified types of record-keeping systems through a public rule-making process that gives interested individuals and groups an opportunity to express their views and, if necessary, to engage the agency in a public debate on the proposed exemption at issue.

Agency responsibility and accountability for compliance with the Act's requirements are also reflected in the approach taken to remedies. Criminal penalties are provided for willful concealment of the existence of a system of records as well as for unauthorized disclosure of personal information. But the principal sanctions are the rights of an individual to seek injunctions, to bring suits and, in some instances, to recover damages from an agency that fails to treat his record properly.

Challenges and Opportunities

One of the most difficult near-term tasks will be the achievement of a sufficient degree of coordination among the various management functions necessarily involved in the implementation of the Act. These include (in addition to the wide variety of program functions whose information bases are the Act's principal concern) the records management policy function itself, the EDP operations and planning function, the personnel management and training function, budgeting, facilities and services procurement, legal counsel, and whatever other information policy functions may be directly or

* Send 75¢ to the Superintendent of Documents, U. S. Government Printing Office, Washington, D.C.

CONTINUED

2 OF 3

potentially affected by the implementation of the Act—for example, those concerned with the administration of the Freedom of Information Act and with the handling of classified information.

Second, because of the centrality and detail of the annual public notice requirement, and because of the substantial criminal and civil penalties for willfully failing to comply with it, agencies have had to undertake a full-scale inventory of their personal data holdings. For at least some agencies this has precipitated a searching review of their need for the personal information they maintain, the cost of collecting and maintaining it, and the way in which their various holdings are distributed. The result should be a heightened awareness of the role of personal-data record-keeping policies and practices in the performance of agency functions. It may also lead to some interesting developments in the methodology of information policy-making, including some needed work on cost-accounting and budgetary implications of agency record-keeping practices.

Third, it is clear that the provisions of the Act requiring agencies to permit an individual to have access to a record about himself will raise some practical questions about the organization of record-keeping functions, including the cost and control consequences of varying degrees of decentralization.

And **fourth,** one can probably expect to see a certain amount of attention focused over the next few years on the incentives that exist or might be developed within agencies to assure that agency officials and employees comply with the spirit as well as the letter of the Act.

On the study and research side, the empirical value of the Act's various documentation requirements, and most notably of its public notice requirement, are obvious. To the extent that records and record-keeping policies and practices reflect the way in which government programs actually operate, the Privacy Act will produce an unprecedented wealth of raw material for the student of government organization and management.

Federal experience under the Act will also be of substantial and continuing interest to law makers and administrators at the State and local level and to organizations in the private sector. Section 5 of the Act establishes a two-year, independent, Privacy Protection Study Commission to consider whether the Congress should entertain similar legislation affecting State and local government and the private sector. Through its study and review of a wide range of public and private records systems, and its analysis of their impact on individual liberties, institutional relationships, property rights, and standards of professional ethics, the Commission will make general recommendations and propose changes in laws and regulations. Meanwhile, however, one can continue to expect considerable attention to be paid to the issue in State Legislatures.

Ideally, a systematic means will gradually be developed for appraising the effectiveness of the Act both as a protection for individual citizens and as a device for improving the quality, organization, and utility of the information that government agencies collect and maintain about people. Is it meaningful, in practice, to speak of obtaining an individual's voluntary assent to the collection and disclosure of information about him in a government record? Does a policy of allowing individuals to interact with records about them lead to improvements in the accuracy, timeliness, and relevance of information in the records? Is it possible to make explicit and codify the uses that are made of recorded information **within** an organization or are the patterns of circulation and use so various and unstable as to defy systematic exposition?

To what extent can the concepts, requirements, and administrative mechanisms in the Federal Privacy Act be usefully applied in other non-Federal and non-governmental settings? Can one find alternative approaches in State government and the private sector which look different, but do at least as good a job of assuring that records about people are handled in ways that adequately protect their important right to personal privacy?

These are all intriguing and important questions. And the Privacy Act of 1974 should help us to address them with much greater confidence than has heretofore been possible.

☆ U.S. GOVERNMENT PRINTING OFFICE: 1976 O—579-820