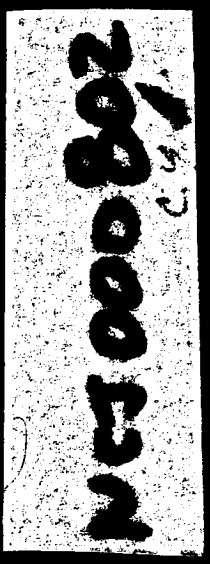
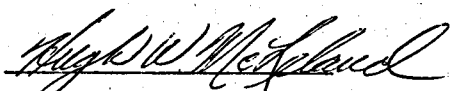


SECURITY AND PRIVACY CONSIDERATIONS IN CRIMINAL HISTORY INFORMATION SYSTEMS

Approved for Publication:

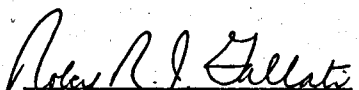
Emery Barrette



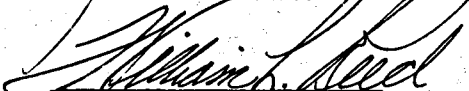
Hugh W. McLeland

C. J. Beddome

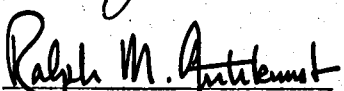
James N. O'Connor



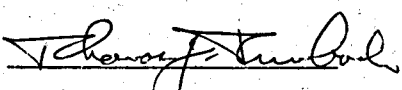
Robert R. J. Gallati



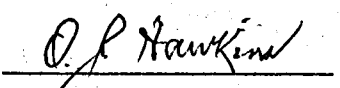
W. L. Reed



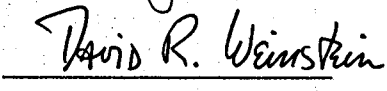
Ralph M. Gutekunst



Thomas Trimbach



O. J. Hawkins



David R. Weinstein

Published By:

Project SEARCH Staff
California Crime Technological
Research Foundation
1108 14th Street
Sacramento, California 95814

Material in this report has been derived from the efforts of all project personnel.

PROJECT GROUP

Orville J. Hawkins, Chairman, California
Thomas J. Trimbach, Vice Chairman, Michigan

Emery Barrette, Minnesota
C. J. Beddome, Arizona
Robert R. J. Gallati, New York
Ralph M. Gutekunst, Maryland
Hugh W. McLeland, Texas
James N. O'Connor, Washington
William L. Reed, Florida
George B. Trubow, Maryland *
David R. Weinstein, Connecticut

STANDARDIZATION TASK FORCE

Edward T. Mattson, Chairman, Minnesota
Philip G. Tannian, Vice Chairman, Michigan

Wesley R. Barrett, California
Robert M. Beck, Arizona
Jerome J. Daunt, Washington, D.C.
Sue S. Johnson, New York
Donald F. King, Florida
Mark A. Levine, Maryland
Dexter B. Lyman, Connecticut
James A. McCafferty, Washington, D.C.
Paul D. McCann, New York
H. W. McFarling, Texas
Edward D. Miller, Connecticut *
DeWitt Whitman, Washington

STATISTICAL METHODS TASK FORCE

Glenn Dafoe, Chairman, Michigan
Willard H. Hutchins, Vice Chairman, California

Kelley Ballard, Washington
Jerome J. Daunt, Washington, D.C.
Charles M. Friel, Texas
Charles Graham, Arizona
Ralph M. Gutekunst, Maryland
Donald F. King, Florida
Nathan Mandel, Minnesota
Wayne R. Mucci, Connecticut
Vincent O'Leary, New York
Charles E. Robinson, New York
John G. Yeager, Pennsylvania

STATE PROJECT COORDINATORS

Lloyd Bastian, Florida
Ronald Beattie, California
C. J. Beddome, Arizona
Page Carter, Washington
Adam D'Alessandro, New York
James R. Donovan, Maryland
Harold P. Higgins, Minnesota
Peter Kleck, Texas
Edward O'Brien, Connecticut
John R. Plants, Michigan
Blair I. Shirk, Maryland *

PROJECT COORDINATION STAFF

Paul K. Wormeli, Project Coordinator
Robert L. Marx, Technical Coordination
George A. Buck, Administrative Coordination
Steve Kolodney, Statistical Coordination

TELECOMMUNICATIONS WORKING GROUP

Robert L. Marx, Staff Coordinator, California

David Fergason, Michigan
Donald F. King, Florida
Charles E. Robinson, New York
Joseph Ryan, Arizona
R. L. Smith, California
Michael Stump, Minnesota
John Wunderlich, Maryland

DATA BASE PREPARATION WORKING GROUP

Robert L. Marx, Staff Coordinator, California

Glenn Dafoe, Michigan
Elmer Hauge, California
Donald King, Florida
Joseph Oliver, New York
Joseph Ryan, Arizona
Larry Hedin, Minnesota
Warren Hansen, Maryland

STATISTICAL ADVISORY COMMITTEE

Vincent O'Leary, Chairman, New York

Ronald Beattie, California
Charles Friel, Texas
Ralph M. Gutekunst, Maryland
Donald King, Florida
James McCafferty, Washington, D.C.
Paul Sylvestre, Washington, D.C.

LAW ENFORCEMENT ASSISTANCE ADMINISTRATION PARTICIPANTS

Lewis Arnold
Melvin Axilbund
Clarence Coster
George Hall
Charles Kinderman
Patricia Rowen
Alfred Sansone
Daniel Skoler
Paul Sylvestre
Anthony Turner
Richard Velde
Paul Woodard

* Past members.

ACKNOWLEDGMENT

The basis for this report is Report No. 1 of the Committee on Security and Privacy, submitted and accepted as a working document on May 25, 1970. The SEARCH Project Group wishes to acknowledge the vigorous and dedicated efforts of the committee and its consultants in producing this important report for the Project SEARCH participants.

The committee members include:

Robert R. J. Gallati, Chairman, New York
Emery Barrette, Minnesota
C. J. Beddome, Arizona
George F. Hall, Washington, D.C.
H. W. McFarling, Texas
David Weinstein, Connecticut

TABLE OF CONTENTS

Chapter 1
Introduction

This report is designed to serve as a reference on matters of security and privacy for all those individuals who may participate, observe, assess, or otherwise become involved in the demonstration of Project SEARCH or the development of a future system for an interstate exchange of criminal histories.

Project SEARCH, an acronym for *System for Electronic Analysis and Retrieval of Criminal Histories*, is funded by the participating states and the Law Enforcement Assistance Administration (LEAA). LEAA was established in the Department of Justice to administer funds provided under the Omnibus Crime Control and Safe Streets Act of 1968, 82 Stat. 197.

The specific objectives of this report are:

1. To construct a fundamental working document that enumerates potential security and privacy problems and presents solutions for the guidance of participants in Project SEARCH during the demonstration period.
2. To provide a dynamic framework of essential elements of security and privacy for any future national system which may develop as a result of Project SEARCH.
3. To outline the kinds of security requirements and self-imposed disciplines that the participants have, by their own initiative, levied upon themselves and their colleagues in Project SEARCH.

I. Background

To develop a proper context for the discussion of security and privacy issues, four major background statements are pertinent:

1. The requirement for a computerized national system for exchanging criminal history data.
2. The system concept being tested by Project SEARCH as a prototype.
3. The security and privacy issues relevant to this system.
4. The Project SEARCH response to these issues.

The intention in this section is to provide a reasonably concise review of these four points.

Requirements for a National System

Criminal justice agencies frequently require, in making decisions regarding a suspect or offender, knowledge of his prior involvement with the criminal justice system. The specific data needs vary in both content and urgency, but the general need is for information about prior arrests, court dispositions, and correctional involvements and outcomes.

A partial, manual system currently exists that supplies some of the information needed. Fingerprints submitted to the FBI and to some of the states in conjunction with a criminal justice transaction (e.g., arrest or incarceration) are used as a basis for recording these transactions on a *rap sheet.* The rap sheets maintained and distributed by state agencies and the FBI generally contain complete listings of arrests and prison admissions, as these two processes regularly involve fingerprinting.

The FBI and most state identification bureaus attempt to collect court disposition data for inclusion on the rap sheet, which is then available for responses to inquiries concerning offenders.

The manual system suffers in two respects. First, the national system is voluntary, with the national coverage fulfilled only by the FBI, in performing a service to contributors. The lack of mandatory reporting limits file completeness. Second, the elapsed time to obtain the criminal history data through the mail is measured in days or weeks in most places and is, therefore, not useful in police or court actions which must be completed in minutes or hours.

The specific functional areas requiring timely and complete information on a national basis are spread throughout the criminal justice system. Beginning with law enforcement, for example, in most police "on-scene" investigations where possible suspects are involved, the officer requires immediate knowledge of prior record to aid in making decisions regarding search, detention, or arrest.

Given factual knowledge of the occurrence of a crime and that the suspect was in the vicinity, the law enforcement officer's aim is to obtain sufficient information to determine the extent to which further police investigation should be conducted. For this purpose, it is necessary to quickly supply the investigator with sufficient data to pursue the case in an intelligent manner. Further information about the suspect is vital knowledge for the officer charged with arresting the subject; for example, does he have a record of violent behavior or of using lethal weapons?

Aside from the value of rapid response in an on-the-scene investigation or imminent arrest situation, a rapid and complete nationwide record search would assist the police in proper charge determination. It would also support procedures enabling the police to issue a summons, in certain cases, in lieu of a formal arrest and possible detention. More complete and timely criminal histories will also help police determine court jurisdictions and make other decisions concerning bail, alert them to an arrestee's present criminal justice status (e.g., whether he is on release pending trial, or is on probation or parole), and provide additional investigative leads and data valuable for effective interrogation.

A prosecuting attorney could benefit by more timely and complete data in those cases, for example, where there is a lapse of time between arraignment and trial during which the accused has been free on bail and has been involved in some other criminal activity. Further, information on a previous criminal offense committed in another part of the country might be received before initial arraignment or grand jury proceedings rather than afterwards, as is now often the situation. The case of an active, mobile check passer is a good illustration of the kind of situation when rapid access to complete data is likely to be of assistance.

Probation officers would be materially assisted in evaluating whether an offender should be "released on his own recognizance", since rapid notification of the nature of an offender's previous record may play a principal role in this determination. In the absence of adequate information, a prosecutor is likely to recommend, and a court will be inclined to set bail at a "safe" level in order to hold the defendant—often in cases where he might well be released pending trial. Indeed a prudent judge might have no other choice since he has no knowledge of the defendant other than what is presented to him at the bail hearing. He "errs" on the safe side of community protection, unless informed.

In addition, both the probation officer and the court should receive timely notice of a probationer's arrest for a new offense, since the arrest usually requires reconsideration by the court of the probationer's program or status. Similarly, parole officers and correction officials are directly concerned when a parolee commits a new criminal act; any new arrest while on parole—whether felony or misdemeanor—is sufficient reason for review of the parolee's program and may be cause for his return to the penal institution.

To satisfy these needs, an improved system would have to have the complete data available only through a national system. Local criminal justice agencies serve limited population and geographic areas; but the population is increasingly mobile. Although a large police agency may contain the criminal records of 1,000,000 individuals and a medium-sized agency may hold records of only 7,000 individuals, both records systems are affected by criminal mobility.

A study in New York State demonstrated the extent and consequence of this mobility. In one large up-state city, almost 30 percent of the persons who have been arrested one or more times for fingerprintable offenses have arrest records in other jurisdictions within the state. The problem is even more acute for chronic offenders; in the same city approximately 55 percent of persons arrested two or more times have records in other in-state jurisdictions. For the state as a whole, the respective percentages for the "average" jurisdiction are 29 percent and 47 percent. Although the percentages may decrease as the geographical area is increased, there is still a substantial degree of mobility in regional and national terms.

There are many other situations in carrying out criminal justice functions that could benefit by the rapid availability of criminal history information. A complete analysis of this requirement is beyond the scope of this report. It is clear that a system is required that will provide a means of determining the nature of prior criminal involvement, in time to be useful for some of the critical decisions related to arrest and prosecution.

Project Search as a Prototype

These operational factors have led to the conclusion that a national system is necessary, and that it must be computer-assisted to achieve the needed responsiveness. The need for this system has been recognized for some time. For example, the President's Commission on Law Enforcement and the Administration of Justice spoke of the need for "an integrated national information system". Specifically, the Commission recommended that "there should be a national law enforcement direc-

tory that records an individual's arrest for serious crimes, the disposition of each case and all subsequent formal contacts with criminal justice agencies related to those arrests".

Project SEARCH was begun in July of 1969, with 10 states * participating. The main goals of Project SEARCH are to:

- Evaluate the technical feasibility and operational utility of a cooperative interstate transference of criminal history data.
- Demonstrate the capability to automate state-collected criminal statistics for retrieval by selected state and federal agencies.

The system concept is based on the maintenance of individual state-held files and the existence of a central index, directly accessible by users in each state and containing summary data on each state-held file. The central index will respond to an inquiring terminal by providing personal descriptors and identifying numbers, an abbreviated criminal profile, and the name of the state or agency holding the full criminal history record (Agency of Record). The requesting state may then directly access the desired file from the Agency of Record.

The system concept also contemplates that when a transaction takes place between an offender and an agency in a state other than the Agency of Record, that state becomes the Agency of Record, the criminal history file is transferred from the previous Agency of Record, the file is updated, and the central index is updated to reflect these changes.

The full criminal history files maintained by the Agency of Record will include a set of required data plus other optional data required for internal state use. The recorded data includes a minimum set of personal descriptors and identifying numbers, and a record of each criminal justice transaction between the offender and the involved criminal justice agencies. These transactions (for felonies or gross misdemeanors) may include information on and outcomes of arrest, pre-trial hearing, trial, sentencing, and correction including probation/parole.

The central index, containing a count of arrests and convictions by major offense category, is designed to be sufficient for answering inquiries by officers in the field needing a quick response as to whether or not a person was in the system (has a prior record) and some brief indication of prior offenses. The index "points" to a state file which is designed primarily to allow other less urgent needs to be satisfied. The state file indicates dates and agencies where the subject has had prior involvement with the criminal justice system, thereby allowing a more refined "pointer" for obtaining further information.

The intent is that the criminal summary contained in the central index could satisfy over half of the inquiries, avoiding the second inquiry to a state. The state inquiry should then satisfy a major portion of the remaining needs, minimizing the effort required in contacting numerous local agencies for more detail on the offender.

To test the feasibility of this system concept, a prototype is being constructed. Seven of the ten SEARCH states are each converting approximately 10,000 criminal histories for loading into the central index, and also creating the more detailed computerized file in their own state.

The Project SEARCH system is designed so as to permit remote terminal access only by personnel of government criminal justice agencies, for purposes associated with official criminal justice functions.

* Arizona, California, Connecticut, Florida, Maryland, Michigan, Minnesota, New York, Texas, and Washington. Colorado, Illinois, New Jersey, Ohio, and Pennsylvania have also been designated as "official observer states".

The prototype system will be demonstrated during July and August of 1970. An evaluation period will follow, and recommendations will be made regarding the feasible development of an ongoing, fully operational, nationwide system.

Security and Privacy Issues

It is essential to clearly and carefully identify the specific issues related to system security and rights of personal privacy that should properly be associated with the design and operation of a nationwide system for access to criminal history data. The logical and rational development of procedures which ensure a reasonable protection of individual rights of privacy, while maintaining the capability required by criminal justice agencies, will lead to a more credible and useful system. Conversely, a lack of attention to correctly stated issues is likely to produce confusion in the system purposes and procedures, and to diffuse the benefits which could be gained by having an operational system.

It is important to point out that the discussion of security and privacy issues follows the basic assumption that some kind of a national system is essential. Within that context, the issues can then be described in terms of implications for the system.

From an operational point of view, there are three basic problem areas that are relevant to security and privacy:

- Unintentional errors. Ranging from typographic errors to mistaken identities, there is always the possibility that the data finally stored in the system will be incorrect, without any intent to make it so.
- Misuse of data. Information can be used out of context or for purposes beyond the legitimate criminal justice functions, both by persons who are actually authorized access and by those who acquire the information even without authorization.
- Intentional data change. The data maintained can be destroyed or modified to accomplish the same objectives as described under misuse, or to restrict the proper and effective performance of criminal justice functions. It has been suggested that organized crime may attempt to penetrate the system for this purpose.

The critical point here is that these problems are not unique to a computerized criminal history system, or even to criminal justice. The same problems exist with all partly sensitive public records. The police agencies throughout the country and the FBI have long recognized the need to carefully control the records under their cognizance. The FBI and state identification bureaus generally refuse, except where required by law, to divulge information in their files to persons not connected with the criminal justice system. Every effort is made to insure that the final positive fingerprint-based identification is performed prior to the release or application of information contained on the existing criminal rap sheets.

Therefore, the fundamental issues to be addressed in Project SEARCH, and in any subsequent nationwide system, are not just related to these problem areas, but rather to: (1) the degree to which the consequences of these problems are substantially different, and (2) the

extent to which these problems will be more prevalent, when a computer with its associated high-speed response and remote access capability is part of the system.

If the use of a computer does not substantially alter the consequences of unintentional mistakes or substantially increase the opportunity for misuse or data changes, then there would not be a requirement to develop policies and procedures in any more detail than for the manual system.

The provision of remote-terminal, fast access has two effects—a dramatic increase in the number of persons and agencies who can obtain the data, and a highly probable increase in the actual number of inquiries. The ease and speed of access will unquestionably cause more inquiries and thereby place more data in the hands of the increased number of users. Remote terminals also make it more difficult to control individual access, as the system is generally only able to identify terminals and not operators. While it can be argued that this is no different than controlling access to a mail room, in a sense, it is physically and mechanically simpler to gain access to a terminal, particularly if it is unattended and the operating instructions unsecured.

Given these possibilities, then, are the consequences or likelihood of occurrence (of the problems mentioned earlier) affected?

Taking the problem of mistakes, it should first be pointed out that the recording and processing discipline associated with the use of a computer is likely to reduce the frequency of unintentional error. Many errors not caught are allowable to a manual system, but will inhibit the operation of a computer system. However, the consequences of some types of errors may be substantially amplified simply by the fact that there are many more persons with access and the system response speed may exceed the error detection and correction speed.

The possibility that the data will be misused may increase substantially over a manual system, also, because of the increase in users and the easy access, unless controls are implemented. The computer itself introduces more opportunities for misuse. For example, a computerized file can be quickly searched by whatever data elements it contains, such that compilations of subjects can be prepared with respect to certain characteristics contained in the file.

The opportunity for intentional modification or destruction of records is increased in proportion to the file centralization of the system. A disc or tape file is much more vulnerable to undetectable modifications by programming or other means than the more inefficient dispersed paper file.

Because of these factors, it is clear to the Project SEARCH participants that the use of a computer as a basis for the system produces a fundamental, substantive change in both the possibility and consequences of possible problems. Accordingly, there must necessarily be a reconsideration of the controls to be imposed on the system, particularly with respect to the security of records and in association with the preservation of reasonable rights of individual privacy.

Project SEARCH Actions on Security and Privacy

In response to this perceived significance of a new technological approach to the criminal history file, the participants in SEARCH have

undertaken a program to address the security and privacy issues. During the initial organization of the project, a *Security of Records Subcommittee* was formed under a Standardization Task Force to deal specifically with this issue. This subcommittee was chaired by Chief H. W. McFarling of the Data Processing Division of the Texas Department of Public Safety. Other members included Inspector Jerome Daunt of the Federal Bureau of Investigation, and Mr. Philip Tannian of the Wayne County Prosecuting Attorney's Office in Detroit, Michigan.

The subcommittee was responsible for providing initial research and a general analysis of the security and privacy implications on the project. Their recommendations for a future course of action were presented to the Project Group (the policy-making body of the project).

This group created a *Security and Privacy Committee* to review and carry forward the recommendations of the subcommittee. Dr. Robert Gallati, Director of the New York State Identification and Intelligence System, was appointed Committee Chairman. Other members included Emery Barrette, Executive Director of the Minnesota Governor's Commission on Crime Prevention and Control; George Hall, Director, National Criminal Justice Statistics Center, LEAA; Captain C. J. Beddome of the Arizona Department of Public Safety; Chief H. W. McFarling; and David Weinstein, Executive Director of the Connecticut Planning Committee on Criminal Administration.

The committee immediately began to explore the specific issues related to the development of a computerized criminal history system and to identify the problems that should be addressed.

The initial review of the problem areas which the committee would have to investigate brought forth a number of recommendations which were implemented. Among these were:

- The decision to draft a Code of Ethics.
- A recommendation that consultants be hired.
- A resolution to limit the information content of the central index.
- Acceptance of the principle of post-auditing.
- Identification of specific questions that required policy decisions.

The Project Group authorized the committee to select appropriate consultants to assist the members in their studies and the preparation of this report. The selected consultants were: Professor Charles Lister of Yale University Law School, and Mr. Jerome Lobel of Ernst & Ernst, Phoenix, Arizona.

The committee has produced three major documents to date—the Code of Ethics (Appendix A), a set of procedures concerning security and privacy which were included in the SEARCH Operating Manual, and this report. Several additional tasks are currently in progress or planned for consideration:

- *Development of Model Administrative Regulations and Statutes*
  The committee is presently studying model legal statutes for the participant states and model administrative regulations for participant agencies. The conflict and diversity of legal structures supporting the identification function in the various states need to be reconciled for purposes of uniform requirements relating to security and privacy. Likewise, federal and state administrative

regulations need to be standardized so that they are uniformly protective of civil liberties.

- *Continuous Audit*
  Project SEARCH is committed to the concept of continuous pre- and post-audit of its activities by an independent group in order to check accuracy and reliability and detect discrepancies so as to permit adjustment of procedures and safeguards accordingly. The Project Group has agreed to the need for review by responsible persons outside the system itself as an essential check on the system, and the committee is presently exploring alternative mechanisms for this process.
- *Evaluation and Feed-Back*
  The committee is currently considering the various methods that should be utilized for continued monitoring, evaluation, and feedback of matters relating to security and privacy. A recommendation has been made by the committee that this consideration be made an integral part of the formal evaluation of Project SEARCH.
- *Education and Training for Participants*
  The committee is currently mapping out an extensive educational program for all Project SEARCH participants. To the extent possible, information concerning security and privacy will be incorporated in the various demonstration and operation manuals. Similarly, this report and various brochures derived from it will serve to inform participants about maintaining a system that meets the proposed security and privacy standards.

II. Scope of the Report

The study results and recommendations which follow represent the major initial results of the effort expended by the Security and Privacy Committee. In keeping with the objective of providing material which will be of value to those engaged in either the Project SEARCH demonstration or in designing a subsequent national system, the remainder of this report has four basic parts: a list of recommended policies, a discussion of the various aspects of privacy, a discussion of system security, and a set of pertinent appendices.

- *Recommendations*
  Chapter 2 presents a set of recommended policies for consideration both in Project SEARCH and in any future system. These recommendations have been approved by the SEARCH Project Group.
- *Legal Aspects of Privacy*
  Chapter 3 contains a detailed discussion of many of the design, procedural, and organizational aspects of the system as they affect personal privacy. General approaches are suggested to ensure that the issues raised are not overlooked in present and future plans.
- *System Security*
  Chapter 4 turns to the operating system itself—equipment, software, and operating procedures—to describe controls and precautions that relate both to ensuring reasonable rights of privacy and protecting system data.
- *Appendices*
  The major appendix is the Code of Ethics, which has been specifically approved for publication by the SEARCH Project Group and

first appeared in the Project SEARCH newsletter. A glossary and bibliography are also provided.

Basically, the chapters following the recommendations attempt to analyze and recommend solutions to problems and issues that the committee has identified initially as being of sufficiently serious long-term consequence to require immediate attention. The committee believes that there need not be a conflict between the safeguarding of reasonable rights to privacy and the construction of a shared information system such as Project SEARCH, if the following potential problem areas are given adequate consideration:

1. The types of data that will be contained in the computerized files.
2. The persons who will receive the data.
3. The purposes for which the data will be used.
4. The relationship between the system and the people whose criminal history records comprise the data bank.
5. The organizational and administrative aspects of the system.

The remainder of this report addresses these considerations.

Finally, the most fundamental philosophical problem underlying the challenge of providing adequate security and privacy for Project SEARCH is one of a balancing of values. The need for an informed, effective criminal justice system must be balanced against the need for an individual to keep information about himself and his life private.

The committee is dedicated to the enhancement of both individual freedom and effective criminal justice. One need not be sacrificed for the other. As new levels of progress are achieved, the delicate balance so essential to a just society will find equilibrium.

It is in this spirit, based on an understanding of the dynamics of both society and technology, that the committee submits this report as a frame of reference for a correspondingly dynamic concept of security and privacy policy with respect to criminal history information systems. There is every intent herein to encourage further progress in the development of this concept beyond what time and resources allowed, and in conjunction with the progress in the development of improved aids for criminal justice agencies.

Chapter 2
Recommended System Policies Related to Security and Privacy

The following list comprises those specific points that the committee believed to be important enough to establish a policy early in the development of a final system concept. Although one of the direct tasks of the committee was to propose procedures for inclusion in the Project SEARCH Operating Manual that would be used during the demonstration, it was very difficult to prepare procedures in the absence of general policies regarding a total system. It became apparent that a set of major policy statements had to be derived as an initial starting point for the procedures relative to the demonstration. Although it is not always easy to determine which policies could be directly implemented for a two-month demonstration, there was general agreement regarding the long-range issues to be treated.

The Project Group officially approved these statements of recommended policy, and the procedures stipulated in the Operating Manual are based on this list.

The reasoning behind each recommendation is presented in the discussions of the following chapters, and a page is cited for reference to the appropriate discussion, where the context is explained. The recommendations are grouped into categories related to later discussion sections.

RECOMMENDED POLICY

Data Content

1. Data included in the system must be limited to that with the characteristics of *public record*, i.e.: (Reference pages 16–18)
   a. Recorded by officers of public agencies directly and principally concerned with crime prevention, apprehension, adjudication, or rehabilitation of offenders.
   b. Recording must have been made in satisfaction of public duty.
   c. The public duty must have been directly relevant to criminal justice responsibilities of the agency.
2. Participants shall adopt a careful and permanent program of data verification: (Reference pages 19–20)
   a. Systematic audits shall be conducted to insure that files have been regularly and accurately updated.
   b. Where errors or points of incompleteness are detected, the Agency of Record shall notify the central index (if necessary) and any participant to which the inaccurate or incomplete records have previously been transmitted.
   c. The Agency of Record shall maintain a record of all participants that have been sent records.
   d. Within a state, a record should be kept of all agencies to which the system's data has been released.
   e. All known copies of records with erroneous or incomplete

information shall be corrected.

3. Purge procedures shall be developed in accordance with the Code of Ethics. Each participating agency shall follow the law or practice of the state of entry with respect to purging records of that state. (Reference page 20–22)
4. A model state statute for protecting and controlling data in any future system should be drafted and its adoption encouraged. (Reference pages 34–37)

Rules of Access and Data Use

5. Direct access to the system should continue to be restricted to public agencies which perform, as their principal function, crime prevention, apprehension, adjudication, or rehabilitation of offenders. (Reference pages 23–28)
6. Definitional questions as to users should be presented for resolution to representatives of all the participating states in the system. (Reference pages 23–28)
7. In order to limit access, the following restrictions should be made: (Reference pages 26–27)
   a. Participating states should limit closely the number of terminals within their jurisdiction to those they can effectively supervise.
   b. Each participating state should build its data system around a central computer, through which each inquiry must pass for screening and verification. The configuration and operation of the center should provide for the integrity of the data base.
   c. Participating agencies should be instructed that their rights to direct access encompass only requests reasonably connected with their criminal justice responsibilities.
8. Requests from outside the criminal justice community to examine data obtained through the system should be honored only if the receiving agency is authorized access by local law, state statute, or valid administrative directive. Efforts should be made to limit the scope of such requirements. (Reference pages 26–27)
9. The security and privacy staff should study various state "public record" doctrines and begin prompt efforts to obtain appropriate exemptions from these doctrines for the system's data. (Reference page 27)
10. The use of data for research shall involve the following restrictions: (Reference pages 32–34)
    a. Proposed programs of research should acknowledge a fundamental commitment to respect individual privacy interests.
    b. Representatives of the system shall fully investigate each proposed program.
    c. Identification of subjects should be divorced as fully as possible from the data.
    d. The research data should be shielded by a security system comparable to that which ordinarily safeguards system's data.
    e. Codes or keys identifying subjects with data should be given special protection.
    f. Raw data obtained for one research purpose should not subsequently be used for any other research purpose without consent of system's representatives.
    g. Security and data protection requirements should be included in any research contract or agreement.

h. Non-disclosure forms should be required and the system should retain rights to monitor and, if necessary, terminate any project.

Data Dissemination

11. Data received through the system should be marked and readily identifiable as such. (Reference page 27)
12. Heads of agencies receiving information should sign a copy of an appropriate recommended non-disclosure agreement. (Reference page 32)
13. Educational programs should be instituted for all who might be expected to employ system data. (Reference page 30)
14. Users should be informed that reliance upon unverified data is hazardous and that positive verification of identity should be obtained as quickly as possible. (Reference pages 30–31)
15. Users should be clearly informed that careless use of this data represents unprofessional conduct, and may be subject to disciplinary actions. (Reference pages 30–31)
16. The central computer within each state, through which all data inquiries should pass, will screen all inquiries to exclude those that are inconsistent with system rules. (Reference pages 26 and 34)

Rights of Challenge and Redress

17. The citizen's right to access and challenge the contents of his records should form an integral part of the system consistent with state law. (Reference page 28)
18. Civil remedies should be provided for those injured by misuse of the system where not provided for by state law. (Reference pages 36–37)

Organization and Administration

19. The system participants should elect a board of directors (governing body) to establish policies and procedures governing the central index operation. (Reference pages 36–37)
20. The system should remain fully independent of noncriminal justice data systems and shall be exclusively dedicated to the service of the criminal justice community. (Reference page 26)
21. A permanent committee or staff should be established to consider problems of security and privacy and to conduct studies in that area. (Reference page 35)
22. The permanent staff should undertake a program to identify differences among the states in procedures and terminology, and to disseminate information concerning them to all participants. (Reference page 35)
23. A systems audit should be made periodically by an outside agency. (Reference page 20)

Chapter 3
Legal and Operational Aspects of Privacy

The scope of this chapter is designed to address the legal, organizational, and administrative guidelines relating to the protection of individual privacy. Computer system security is addressed in the next chapter. The intent here is to provide an explanation of the rules that have been adopted for the Project SEARCH prototype demonstration, to discuss the considerations pertinent to the design of any subsequent system, and to explore the consequences of significant variations in or additions to the demonstration system.

I. Scope of the Files

The first and often most fundamental questions about any information system involves the nature of the information it will include. No one can deny government's right to collect and employ information about its citizens; to do so would condemn many governmental activities to inefficiency and perhaps uselessness. The privacy issues instead turn on the quality, character and intended uses of the data that are to be collected.

The Project SEARCH demonstration is built upon a series of interconnected restrictions. These restrictions encompass both the classes of persons about whom data are to be collected and the kinds of information that are to be sought. The persons to be included in the file of the central index may be only those for whom at least one charge has reached a final disposition and for whom a Federal Bureau of Investigation number has been assigned. The temporary decision concerning FBI numbers will be reviewed following the demonstration, and a permanent decision made at that time.

The information to be included in the state-held Project SEARCH files is a record of each of the individual's major steps through the criminal justice process. The information held in the central index will be even more narrowly restricted. The index will serve merely a directory function and will include only identifying data, the location of the Project SEARCH state file, and a bare summary of arrests and convictions.

The Code of Ethics, which is attached to this report as an appendix, makes it clear that information may be collected only upon the report of a crime and the commencement of criminal justice system proceedings. The trigger for beginning to take data is declared by the code to be the recording of arrest fingerprints.

Project SEARCH Criminal History

The computerized criminal history maintained at the state level will

essentially include only the results of each formal stage of the criminal justice process:

- The fact, date and arrest charge; whether the individual was subsequently released and, if so, by what authority and upon what terms.
- The fact, date and results of any pre-trial proceedings.
- The fact, date and results of any trial or proceeding; any sentence or penalty.
- The fact, date and results of any direct or collateral review of that trial or proceeding; the period and place of any confinement.
- The fact, date and results of any release proceedings.
- The fact, date and authority of any act of pardon or clemency.
- The fact and date of any formal termination to the criminal justice process as to that charge or conviction.

These entries, together with their coding and abbreviations, are more fully described in Project SEARCH Technical Report Number One. The report indicates, in addition, which of these entries are mandatory and which are optional for participating agencies.

Finally, the file will include physical and other identifying data:

The subject's full name
Date and place of birth
Sex
Occupation
Race
Height
Weight
Hair color
Features
Skin tone
Identifying marks
FBI number
Social security number
Any operator's license number
Any miscellaneous identifying numbers

These identifying data are also explained in greater detail in Technical Report Number One. It should be understood that Social Security and other identifying numbers are included in the Project SEARCH files in order to complete or verify individual identifications, and not as a device to permit linkages or data sharing with other information systems.

It is important at this point to observe that these data are, in a fundamental sense, matters of public record. They are recorded by public officers, in consequence of public duties, at the conclusion of relatively formal and often public proceedings. Much of this information is already widely available to criminal justice agencies across the country, either through informal exchange arrangements or through the services of the Federal Bureau of Investigation. Moreover, as we will shortly show, much of this information is in many states available for inspection by interested members of the general public. Project SEARCH will provide more rapid, complete, and accurate dissemination of these data.

Data Exclusions

To make the scope of the files quite clear, certain data are specifically excluded in the prototype system design.

First, Project SEARCH excludes information concerning juvenile

offenders, by which is meant the subject was by reason of his age (and not the age of any victim, co-defendant, or other relevant party) tried in a juvenile or family court. The reasons for this exclusionary rule are essentially those which already render much information concerning juvenile offenses confidential in many states; the widespread belief that this may contribute to the ultimate rehabilitation of the juvenile offender or delinquent.

Second, the project participants have excluded misdemeanor drunk and traffic arrests. It is generally believed that additional less serious misdemeanors should be excluded, and some suggestions along these lines were made by the Standardization Task Force. In view of the complications in data conversion, and the importance of distinguishing between file content at the state level and at the central index level, no further restrictions were imposed for the demonstration. However, the Security and Privacy Committee believes that further studies should be conducted to specify inclusion or exclusion of specific misdemeanors in any future system.

Third, the project's Code of Ethics explicitly excludes unverified data such as that emanating from intelligence sources. The intent here is to avoid the use of data resulting from tips, rumors, or second-hand allegations that have not been formally substantiated or derived from official criminal justice proceedings.

These three categories of excluded data were designed both to provide reasonable protection of individual privacy and to prevent the use of unreliable or inconclusive data for purposes of important criminal justice decisions. In combination, they represent a series of fundamental restrictions upon the proper functions of data systems; they should certainly be regarded as essential limitations upon any future system.

Project SEARCH Privacy Implications

It is believed that these restrictions will create a data system that is limited and relatively hazardless. As we have observed, much of the information it will include is the consequence of public proceedings; much of it is already available to criminal justice agencies across the country through the services of the Federal Bureau of Investigation. The demonstration system does not include subjective evaluations (except as to certain physical characteristics) by police, judges, or detention authorities. It does not include intelligence data, unsubstantiated reports or conjectures. Whatever the risks of recording and disclosure errors (and these are discussed below), the demonstration system is restricted to essentially hard data that can and should be thoroughly verified.

In this connection, a brief examination of the doctrine of public records may be instructive. The laws of every state guarantee, and long have guaranteed, the rights of individual citizens to inspect and copy wide categories of public documents. These rules were recently extended by statute to many of the records and documents of the federal departments and agencies. Public records are commonly not defined with any great precision, but in general they include all books, memoranda, and other documents either required by law to be kept or necessary for the effective discharge of a public duty. The various rights of access to these records are intended to permit public surveillance of the

activities of government. It has been argued since the eighteenth century that popular control of government has as its principal prerequisite the general availability of timely and accurate information about the conduct of public affairs. Public business, it has been thought, is the public's business. The terms of these rights of access vary widely among the states, and it should not be supposed that they are free from important exceptions.

Nonetheless, it can at a minimum be said that much of the information included in Project SEARCH would be available from other sources in many states to suitably interested private citizens. This is not a situation without inconveniences and risks, and we urge that out-of-state data obtained through Project SEARCH should be protected from any local public records statutes.

The committee recognizes that the situation could be quite different if the scope or content of the files of a future system were appreciably altered. If, for example, the files of a future system included intelligence data or data that were otherwise relatively unverified, the threats to individual interst, including privacy interests, could be very significant. Important criminal justice decisions about an individual might be predicated in part upon unsubstantiated, possibly inaccurate or incomplete representations in his file. His employment and other oppotunities might be injured. His reputation among his family, friends and associates might be irrevocably harmed. As these hazards became more serious and common, the importance of rigorous constraints upon the dissemination and use of data would markedly increase. If this occurs, it could result in the creation of a far more restrictive set of operating procedures which could be quite costly.

The committee therefore believes strongly that the data included in any future criminal history system should be limited to those with the characteristics of public records. It accordingly recommends that any such system should adhere to the exclusionary rules described above, and that all data in a future system should satisfy the following minimal requirements.

First, the information must have been recorded by an officer or employee of a public agency directly and principally concerned with the prevention of crime or the apprehension, adjudication and correcton of criminal offenders.

Second, the recording must have been made in satisfaction of a public duty or at least must have been essential for the satisfaction of such a duty.

Third, this public duty must have been directly relevant to the criminal justice responsibilities of the agency with which the recording officer is employed or associated.

II. Collection of SEARCH Data

The first operational process in which guidelines are appropriate for providing reasonable protection of privacy is the data system's collection process. It is important at the outset to recognize the reorientation this requires in the responsibilities of data systems. The customary standard for the adequacy of a system's data collection process would appear to be whether that process will produce timely information of

a kind and quantity that will suffice to support the system's various functions. The standard is self-defined, in that it looks inward to the structure of the data system and outward only to the demands of the system's clients. It disregards, or tends at least to disregard, external costs. If, on the other hand, considerations of privacy are thought to be pertinent, a panoply of new values and interests become important, giving attention to the system's subjects as well as to its clients.

A concern for privacy requires that a system's data be accurate and complete, because of the injurious consequences that may follow for the data's subjects. Privacy requires, moreover, that data collection be limited precisely to the information that is justified by the legitimate functions of the data system.

Project SEARCH Data Collection Restrictions

The collection process provided for Project SEARCH is well calculated to satisfy these constraints. The information included in the demonstration system is the product of formal and relatively well-defined steps in the criminal justice process:

Arrest and consequent fingerprinting
Arraignment
Trial
Detention
Parole proceedings
Release

For purposes of the demonstration system, the data will be those already recorded by employees and agents of the participating public agencies.

Data Accuracy

Much more difficult issues arise from questions about the accuracy and completeness of the records included even in the demonstration system. There is every reason to believe that rap sheets, particularly those initiated or updated relatively recently, faithfully record the criminal histories of their subjects. No body of evidence known to the committee suggests that these files are generally or even frequently erroneous.

Nonetheless, it must be candidly acknowledged that inaccuracies are unavoidable in any system involving many thousands of records. Computers usefully supplement human skills, but they cannot surmount altogether human frailties. Even considerations of privacy cannot sensibly require that data systems be perfectly free of error, but they do demand that reasonable steps be taken to reduce and identify inaccuracies.

Steps to achieve complete data accuracy are not possible during the brief demonstration period, but the committee strongly urges the adoption of a careful and permanent program of data verification for any future system.

The committee's work already contains a framework for such a program. The Code of Ethics provides that the accuracy and completeness of the Project SEARCH data should be matters of great concern for all participants. Regular auditing is required. These requirements might be satisfied by any number of administrative and legal arrangements.

The committee suggests that an adequate program of data verification ought to possess the following characteristics.

First, any such program should require participating agencies of record to conduct systematic audits of their files, in a fashion calculated to insure that those files have been regularly and accurately updated. Periodic programs of employee re-education should also be required, such that every record custodian and clerk is fully conscious of the urgency of faithful performance. Appropriate sanctions, as described later in this chapter should be available for those whose performance proves to be inadequate.

Second, where errors or points of incompleteness are detected, the agency of record should be immediately obliged to notify the central index (if the change involves data stored in the index) and any other participating agencies to which the inaccurate or incomplete records have previously been transmitted.

III. Storage of System Data

There are three sets of problems that warrant attention in this regard:

1. Problems involving the security of the data system.
2. Problems of purging and time limitations.
3. The classification of data maintained in storage.

We will examine each of these in turn.

System Security

Technical questions of computer, physical, and personnel security are examined in detail in Chapter 4, which identifies the principal system security issues and describes the various methods now available to reduce those hazards. It is enough for present purposes to emphasize that an effective system security program is an indispensable component of any wider effort to protect the privacy interests of the data's subjects. The two programs serve complementary values and employ interrelated methods.

- The security program is focused inward on the integrity of the data system and the effective performance of its duties.
- The privacy program looks outward to the interests of those about whom data are collected.

An effective security program is thus a necessary but not sufficient condition of an adequate program for the protection of individual privacy.

Data Purging

Much more complex issues are presented by proposals to purge the data system's files at regular intervals. A variety of purposes may be thought to justify purging provisions, and it is well to examine them separately.

The first such purpose is simply to eliminate information that is found to be inaccurate or at least unverifiable. No objection can be made to such a program, although many might quarrel about its timing and application, and it should be an essential ingredient of any future system.

The second possible purpose is to eliminate information that, because of its age, is thought to be an unreliable guide to the subject's present attitudes or behavior. This may certainly present very controversial matters of judgment, but these again are issues that are only indirectly pertinent to the questions now before us.

The third possible purpose goes to the heart of the privacy argument. It is that society ought to encourage the rehabilitation of offenders by ignoring, and permitting them to ignore, relatively ancient wrongdoing. The forcefulness of this argument should not be underestimated. An important part of the opposition to large-scale information systems is the fear that individuals would no longer be permitted to outlive their mistakes, that isolated or immature errors would follow an offender through a lifetime. If this is true, an information system could run counter to much that has been claimed about this country since its beginnings.

These claims have often been exaggerated, yet many youthful offenders may have been permanently disabled by society's memories of their errors. The claim still symbolizes a recognizable national goal. Like most such goals, it is widely believed, even if it is not widely followed. Designers of criminal justice information systems, therefore, should be prepared to take reasonable steps to accommodate their systems to this goal.

The Project SEARCH demonstration does not include any provisions for the purging of older data, but the committee recommends, and the Operating Manual provides, that such arrangements should be an integral part of any future system.

The Operating Manual, developed for the demonstration, provides that records will be removed from the Project SEARCH central index when the agency of record indicates either (1) that the offender is not under correctional supervision and that no additions have been made to the offender's criminal history for a period of time beyond which the likelihood of recidivism is remote, or (2) that a purging of every entry on the history has been ordered by a competent court or executive authority.

These requirements are supplemented by provisions in the Code of Ethics, Article II, Section 2, which endorse the principle of purging, particularly in cases of first offenders. The committee strongly urges each participating agency in any future system to study closely and sympathetically more comprehensive purging rules.

Connected issues are presented by statutes in several states that provide for the erasure of police and court records following acquittal, dismissal or pardon. These statutes are not without ambiguities, but it at least seems clear that they are intended to exclude such records from any consideration whatever, except in subsequent criminal justice decisions. As desirable and farsighted as these statutes may appear, they still must be expected to present important difficulties. Materials thought to be useful in one jurisdiction will, as records circulate through the system, regularly be sent to states in which they may be entirely impermissible.

No fully satisfactory solution is possible so long as state laws continue to differ, but the committee believes that the best answer at present is to ask each participating agency to follow the law or practice of any state

of entry which has adopted purging rules.

If, in other words, the law of the state of entry provides for purging, the data remain subject to withdrawal throughout their circulation.

It must, however, be understood that these rules are necessarily applicable only to data transmitted through Project SEARCH and any future system; any wider application of the purging principle, so as to reach intrastate data or interstate data obtained through the Federal Bureau of Investigation or other sources, is a matter for the judgment of the several state legislatures.

Data Classification

Although the demonstration system will include only public record information, as has already been explained, there still is a need to protect sensitive data and system components.

One of the methods being considered to provide security and privacy protection in Project SEARCH is a form of sensitivity classification.

It has been proposed that a classification index might be developed (similar to the one designed for the New York State Identification and Intelligence System [NYSIIS]). This classification system establishes a quantitative method for defining the degree of sensitivity and, therefore, protection that should be given various classes of information.

The mere fact that Project SEARCH deals exclusively with public record data does not eliminate the need for attention to security and privacy protection, since the data itself becomes fused with system characteristics and cannot be evaluated as to sensitivity as something separate and apart from the system itself.

Thus, the least sensitive data in the substantive sense may become highly sensitive by virtue of the system procedures enveloping it. It is not alone the information that is in the data base that determines sensitivity. Amount and quality of content, where the data is located, who has access, how it is stored, speed and format of retrieval, how and to whom it is disseminated, etc., all are relevant and impact the sensitivity of a system, while the individual capsules of data as such do not in themselves change their character as particular unit items of public record information.

Arguments have been advanced that a statewide data bank of criminal offender records is inherently more sensitive than a local file and that a computerization of the statewide file increases the sensitivity. Carrying such arguments to their logical extreme, a nationwide file, computerized or otherwise, would be more sensitive than a statewide file and a name file would be more sensitive than a fingerprint file. While these questions are subject to debate, if we assume the accuracy of this premise, the security problems increase with the sensitivity.

As an information file progresses from a small, uncoordinated manual file maintained on a local basis through extensive, real-time, on-line nationwide computerized file of the same material, the very possibility for more rapid access and greater correlative activities leads to the probability that a constantly increasing security and privacy protection must also be provided even though the basic unit of information has remained constant. Thus, we must evaluate the data in terms of classification, not necessarily from inherent sensitivity, but rather from a standpoint of available combinations, as they exist in the system.

A minimal classification system would determine the security pattern of processing, storage and transmission, the individuals to whom the data may be disseminated, the manner in which the data must be protected by the recipient thereof and procedures for declassification and/or destruction. Such a classification system should be applicable to all data in the system. An even more comprehensive classification system may be desirable for any future system. This classification system might extend to the data, the various parts of the physical system that processes or stores the data, and all the documentation describing system components and functions. System access and design criteria should also be included in the sensitivity classification.

IV. System Access

Perhaps the most difficult problem, from the standpoint of system design, is that of identifying and controlling proper access to system data. This section addresses the two major categories of access—that of qualified users and that of the offenders whose records are maintained in the file.

Qualified Users

It is important at the outset to emphasize that Project SEARCH data should be used exclusively for the service of the criminal justice community. Project SEARCH represents one of many efforts to employ modern technology to reduce or prevent crime and to help to enforce the criminal law. It was not, and is not now, designed either as a general source of data for government or as a segment of any comprehensive governmental data system. Nonetheless, it must be candidly acknowledged that any such exclusivity of purpose raises many difficult issues of law and policy. A wide variety of demands for Project SEARCH data can be anticipated from outside the immediate criminal justice community.

For reasons, both good and bad, legislators and other state and local officials have increasingly required a criminal records check as a prerequisite for various licenses, occupations, and professions. In many states, applicants for civil service employment, private detectives, taxi drivers, boxing, wrestling and racing personnel, pistol permit applicants, liquor distributors and licensees, applicants for admission to the bar, and many others must have criminal records checks. State and local criminal justice agencies are often required by law to conduct or at least to permit these checks. In addition, the military services, the Federal Bureau of Investigation, and other federal agencies very frequently request access to local criminal records, sometimes for purposes with little direct connection to the criminal justice process.

The comprehensive system of governmental and industrial security clearances depends heavily upon local records. Criminal justice agencies, like the schools, the military services, and the credit bureaus, have become depositories of data upon which an impressive variety of agencies, public and private, seek to draw. It must be expected that such requests would markedly increase if a future system, with all its attendant conveniences, were established.

The committee believes that all such collateral uses of system data should, so far as reasonably possible, be prohibited. It fears that the

widespread use of such data for purposes unconnected with criminal justice might suggest, and indeed perhaps facilitate, the existence of a comprehensive data system that might irrevocably prejudice the concept in the eyes of the general public. Further, any such usage would stimulate very substantial pressures to collect and disseminate categories of data irrelevant for the criminal justice process. The ultimate consequence might easily be the creation of a very different and arguably more hazardous information system. Nonetheless, the committee recognizes that it may well be legally or administratively difficult for some participating agencies to avoid altogether such requests. Committee recommendations are designed to take reasonable account of these constraints.

The first and most important of the committee's recommendations is that direct terminal access to such a system should be restricted to public agencies which have as their principal function the reduction or prevention of crime or the enforcement of the criminal law. Questions of secondary access to data transmitted through such a system are treated later in this section. It will be obvious that difficult questions of definition abound in this area, and that no fully satisfactory solutions can reasonably be expected in this preliminary report.

The array of potential recipients of Project SEARCH information is vast, and each of the potential users might obtain the data in a variety of ways. Potential recipients are both governmental and nongovernmental, as well as persons and agencies that are of the mixed public-private variety. It has been determined that Project SEARCH data would be disseminated in the governmental sector only. However, in the governmental sector itself, we have departments, agencies, commissions, offices, boards, and other units of government, so the question arises whether it is appropriate to disseminate to a single person, a group of persons, or a unit within a larger unit, agency, department, etc. It is entirely possible to have a law enforcement unit, group, or even a single person positively engaged in governmental law enforcement but only as part of a larger organization which is totally unrelated to criminal justice. The most obvious example of this situation is the variety of law enforcement units and criminal justice personnel in the U. S. Treasury Department. In addition, many state conservation departments maintain their own police forces, and law enforcement officials turn up in some of the strangest places at the local level as well.

Some idea of the difficulty encountered in defining a criminal justice officer who might require access to Project SEARCH data can be illustrated by examining the various legal definitions of a peace officer in typical state codes of criminal procedure.

Thus, we find it difficult to define law enforcement officers, law enforcement groups, and organizational units of law enforcement. This kind of confusion is compounded when we broaden our perspectives and attempt to define governmental, individual, group, and organizational units engaged in the administration of criminal justice. Nevertheless, for SEARCH purposes, it was determined that information dissemination criteria would include as recipients only the governmental criminal justice community. The difficulty in arriving at a definition has been encountered by others. For example, the NCIC Advisory Policy Board did not define the term "law enforcement agency" so the difference between "governmental criminal justice personnel, agencies,

and/or units thereof" as defined in this report and "law enforcement agencies" as understood by the Advisory Policy Board may not be as distant as appears at first glance. These questions of definition will undoubtedly prove to be a matter of continuing concern for the participants in any future system. However, the following listings should provide adequate initial guidance.

Under the general standard described above, the following classes of public agencies *may be permitted* direct terminal access to Project SEARCH and any future system:

1. Police forces and departments at all governmental levels that are responsible for enforcement of general criminal laws. This should be understood to include highway patrols and similar agencies.
2. Prosecutorial agencies and departments at all governmental levels.
3. Courts at all governmental levels with a criminal or equivalent jurisdiction.
4. Correction departments at all governmental levels, including corrective institutions and probation departments.
5. Parole commissions and agencies at all governmental levels.
6. Agencies at all governmental levels which have as a principal function the collection and provision of criminal justice information.

The following classes of agencies and individuals would be among those *excluded* from direct terminal access to Project SEARCH and any future system:

1. Noncriminal justice agencies with licensing authorities at all levels of government.
2. Noncriminal justice agencies that are responsible for the enforcement of civil laws at all governmental levels.
3. Noncriminal justice agencies responsible for personnel recruiting or screening at all governmental levels.
4. Public social welfare and service agencies at all governmental levels.
5. Military units and agencies, including military police forces.
6. Courts at all governmental levels without a criminal or equivalent jurisdiction.
7. Private individuals and agencies involved in criminal proceedings, including defense attorneys and legal aid societies.
8. Legislators and representatives of legislatures, legislative committees and councils at all levels of government.
9. Representatives of the communications media.
10. Private individuals and agencies in investigatory occupations, including, for example, private investigators, credit bureaus, and industrial security agencies.
11. All other private agencies and the general public.

The committee recommends that any definitional questions not clearly answered by these listings or by the general standard described above should be presented for resolution to representatives of all the participating states.

Obviously, these rules will exclude from direct access to Project SEARCH and any future system the principal agencies that might be

expected to submit data requests unconnected with the criminal justice process. Nonetheless, a wide variety of secondary restrictions, involving agencies both with and without direct access to the data system, are needed to insure appropriate limitations upon access to the system and to its data.

First are the restrictions upon agencies that may properly be permitted direct terminal access to the system. It should be understood that the above listing is not intended as an authorization for every such agency to establish a direct point of access.

The committee urges each participating state to build its data system around a central computer system, through which each inquiry must pass for screening and verification. This central computer system should have as its special responsibility the monitoring of the usage of SEARCH within the state, and should routinely seek to verify both the identity of the requesting party and, with non-criminal justice agencies, whether or not the requesting party is authorized by law to obtain criminal history records for compliance with its duties. Severe penalties should attach to improper or unauthorized usage. Finally, participating agencies should be instructed that their rights of direct access encompass only requests reasonably connected with their criminal justice responsibilities.

It must be recognized that there are strong pressures to combine and consolidate all state and local data processing into major integrated systems. There are very persuasive and compelling arguments in favor of such integration of data, since, it is argued, the same data elements may be of value to a number of different types of agencies, including law enforcement and criminal justice agencies within a given jurisdiction.

However, the Security and Privacy Committee believes that the SEARCH state data bank should be housed in an existing criminal justice agency capable of properly managing the system within the defined guidelines or in a computer under the operational control of an agency specially created for such purpose and, in either case, independent of any noncriminal justice agency or data file. It has been agreed that no greater number of terminals should be utilized in any state than the state itself is able and willing to vouch for in terms of a level of security and privacy equivalent to that maintained at the state's Project SEARCH computer center.

In accordance with decisions of the Project Group, the telecommunications network filters through the central state data bank. Therefore, each state should be able to maintain control of traffic over the Project SEARCH system network.

We have determined that only governmental criminal justice personnel shall have direct access to the Project SEARCH system. For purposes of demonstration, persons or agencies not classifiable as governmental criminal justice agencies may have access to terminals, but would receive mocked-up data suitable only for illustrating the mechanics of the Project SEARCH operation.

Complex issues may be presented by requests for data from agencies that are denied direct access to the system. The appropriate response to such requests is in principle clear. No use of the system or of data received through the system should be permitted for purposes uncon-

nected with the criminal justice process. Any requests to employ the data for records checks for liquor or taxi licenses, or similar purposes, should normally be declined. Nonetheless, the committee fully recognizes that this principle of exclusivity may readily create severe difficulties for many participating agencies. Public agencies, of course, do not ordinarily segregate their files according to the sources of their data, and important clerical and administrative problems might arise from any obligation to do so. Further, criminal justice agencies are in many states required by law to conduct or at least to permit such records checks. The committee, therefore, recommends that participating agencies should act in accord with the following principles except where state statutes otherwise require:

- Requests from outside the criminal justice community to examine data previously obtained through the system should be honored only if the receiving agency is authorized by local law or valid executive directives to do so. Competent legal counsel should be obtained to determine the limitations of the agency's obligations.
- No inquiries through such a system should be permitted for any purpose unconnected with the criminal justice process. The state's central computer should make every effort to insure that unauthorized inquiries are detected and eliminated.
- Data previously received through the system should be marked and readily identifiable as such. So far as it is administratively feasible, these data should not be intermingled with the receiving agency's other files and documents.

Problems of access are also raised by the statutes under which interested private citizens may inspect and copy wide categories of public documents, sometimes including criminal justice records. The effect of these rights is to offer access to such records to representatives of the communications media, private investigators, credit bureaus, and all other interested citizens. Whatever the wider justifications for the doctrine of public records, the committee has concluded that no such rights of access should be permitted to data obtained through Project SEARCH or any future system.

It, therefore, offers two additional recommendations:

- It believes that the staff of any future system should undertake as one of its first responsibilities a thorough study of the various state public record doctrines. This study should encompass judicial and administrative decisions as well as statutes. It should indicate in which states and with what seriousness the doctrines of public records create difficulties as to system data.
- The committee recommends that participating agencies should begin prompt efforts to obtain appropriate exemptions from these doctrines for future system data. If necessary, statutory relief should be sought. Participants and representatives should be prepared, so far as it is reasonably possible, to assist these efforts. The committee does not assert that these recommendations will eliminate altogether these difficulties; it suggests simply that they represent a realistic and ultimately effective plan of action.

Offender Rights of Access

The second category of access rules involves the possibility of a citi-

zen's right to inspect and challenge the contents of his records. No such provisions were realistically possible in the brief demonstration period, but the committee strongly believes that they should form an integral part of any future system. The reasons are several.

First, an important cause of fear and distrust of computerized data systems has been the feelings of powerlessness they provoke in many citizens. The computer has come to symbolize the unresponsiveness and insensitivity of modern life. Whatever may be thought of these reactions, it is at least clear that genuine rights of access and challenge would do much to disarm this hostility.

Second, such rights promise to be the most viable of all the possible methods to guarantee the accuracy of data systems. Unlike more complex internal mechanisms, they are triggered by the most powerful and consistent of motives, individual self-interest.

Finally, it should now be plain that if any future system is to win public acceptance, it must offer persuasive evidence that it is quite seriously concerned with the rights and interests of those whose lives it will record. The committee can imagine no more effective evidence than authentic rights of access and challenge.

It should be understood that data custodians may take all reasonable steps, including fingerprinting, to assure that access to records under their control is restricted to properly authorized persons.

If the citizen believes that his records are inaccurate or misleadingly incomplete, he should be permitted reasonable opportunities to challenge them. These opportunities might be variously structured, remedies, if they exist, should be used, state statutes could be enacted, or a small number of disinterested private citizens could be asked to serve as members of panels that would conduct informal hearings, take evidence, listen to argument, and formulate specific recommendations.

It will be clear that these procedural guidelines would have to be more clearly and completely defined if the scope of a future system is significantly expanded. A much more complex system of limitations and safeguards would almost certainly be needed. As we emphasized earlier, the committee strongly recommends against any such changes in the character of the information system. If, nonetheless, this occurs, an appropriate system of data categories should be adopted, with varying rights of notice, access, and challenge.

V. Uses of System Data

There are a set of precautions and conditions which are important guidelines to the actual application of data from the system. These guidelines relate to the direct application of data in criminal justice processes, to the potential secondary uses, and to the use of the data for research.

Primary Data Uses

The general types of situations in which criminal history data can be useful were briefly discussed in Chapter 1. Rather than attempt to identify all of the legitimate applications, the concept of primary data uses refers to those situations in which the knowledge of a suspect or offender prior record is of material value to the conduct of the criminal

justice processes. Within this broad definition, however, the nature of the SEARCH system imposes a series of important precautions to be taken in the use of the data. It is acknowledged that Project SEARCH and any future system, like all similar data systems, include risks as well as advantages. The advantages should be obvious to any citizen genuinely troubled by the failures and delays of the criminal justice system. The risks involve increased hazards of mistaken identity as a consequence of the system's increased speed of operation. Although the statistical likelihood of error in any given situation will always remain quite small, the committee believes strongly that these risks should cause serious and permanent concern among participating agencies.

It must be acknowledged that Project SEARCH, as originally conceived, was basically a "name search" system. The addition of an accurate FBI number and other identifiers to the name, of course, makes it possible to be more certain of the identity of the individual. The use of facsimile transmission of fingerprints, as verification of identity, likewise makes positive identification possible. There are, therefore, tradeoffs between speed and certainty of identification. At different intervals in the processing of the offender through the criminal justice agencies that society has created to deal with criminal behavior, there are different requirements for certainty of identification and these are often related to the exigencies of response time.

Prearrest

Through its central index, Project SEARCH seeks to provide immediate basic data concerning the individuals with whom the police must deal at the street level, but almost always on a "name search" basis only. There is no opportunity in on-the-street situations to verify the identity of the suspect in any rigorous fashion. The privacy precaution to be exercised at this point is to ensure that actions are taken in response to factual data, and not merely in light of partially speculative prior record information.

Many police investigations and most prosecuting attorney and grand jury investigations, however, do not require instantaneous response. If the FBI number is known because of prior certain knowledge concerning the suspect; or, if it is possible under the law of the particular state involved to take fingerprints prior to formal arrest, a positive identification may be made and fast responses of summary data obtained from the central index. Shortly thereafter, a more complete record may be requested where desired from the state of record. Both are made possible through the rapid telecommunications and computer interface procedures of Project SEARCH.

It is significant to note that in the first case, records are obtained on the basis of identification other than—and less positive than—fingerprints or their equivalent, or an accurate and certain FBI number (which most often can be obtained only by fingerprinting). The sensitivity of this phase of Project SEARCH operations is critical. It is here that miscarriages of justice could occur because of mistaken identity.

Arrest, Booking, and Arraignment

Arrests are frequently made on the basis of leads obtained through tentative identification; however, it is critical that a prima facie case be

established on facts other than the data obtained from a Project SEARCH response. If the statutory grade of the offense is greater because of the fact of a previous conviction, it is most risky to depend upon a name and personal description search or to take any immediate action in reliance thereon.

With the availability of facsimile and other appropriate means to obtain a positive identification, it should not be necessary to book and arraign and set bail for an individual in reliance upon a criminal history record which is obtained on the basis of a tentative identification. This is not to say that rapid processing is not essential.

Having a charge or bail set too low or too high and the arrestee released or detained before his full circumstances are known, is dysfunctional. On the other hand, unduly holding the arrestee, either by requesting adjournment of the case or by filing a technical charge (such as vagrancy) as an excuse for holding him, compromises an individual's civil liberties. Clearly, these alternatives are a disservice both to the arrestee and his rights and to the local taxpayers who must pay the added costs of criminal justice.

Sentencing, Probation, Correction, and Parole

There is no satisfactory reason why any individual should be sentenced, or be dealt with by rehabilitative agencies, on the basis of a criminal history record obtained through Project SEARCH, unless positive identification of the person has been obtained. Ample time is generally available, in these parts of the process, to obtain positive identification, even using the mail for transmission.

It should be quite clear that positive identification is an essential goal in the general application of SEARCH data.

The committee's first and principal recommendation is, therefore, that participants in Project SEARCH and any future system actively continue to devise more effective methods to minimize every possibility of error. These efforts should be given the highest priority by the staff of any future system. In addition, the following preliminary measures should be implemented by every participating agency in Project SEARCH.

First, a vigorous educational program should be instituted for all police officers, prosecutors, and others who might be expected to employ Project SEARCH data. The program should include frank appraisals of the likelihood and consequences of error. It should remind every officer that prompt and thorough verification must be obtained of every Project SEARCH identification, and that significant criminal justice decisions should be based on unverified data only in the most urgent circumstances. Refresher programs should be repeated at regular intervals.

Second, as indicated earlier, all Project SEARCH data should be marked and identifiable as such. These markings, or a supplementary document that is securely fastened to each Project SEARCH file, should offer prominent warnings that positive verification should be obtained as quickly as reasonably possible and that any reliance upon unverified data is extremely hazardous.

Third, the reports and other documentation routinely completed by police officers should include explicit inquiries about the use made of

Project SEARCH data and the methods employed to verify Project SEARCH identifications. Senior police officers should monitor these and other reports to insure proper usage.

Fourth, police officers and cadets should be repeatedly warned that careless use of Project SEARCH data represents professional misconduct that warrants severe disciplinary measures. Officers who are found to have disregarded these warnings should be thoroughly counseled and, where appropriate, disciplined.

Fifth, prosecutorial authorities should be instructed to make explicit inquiries about the usage and verification of Project SEARCH data in any case brought to them for further proceedings. The absence of positive verification for any identification should be sufficient cause for reconsideration of the case.

Sixth, any reports or documents provided to defense counsel which include Project SEARCH data should routinely describe both the hazards of careless use of the data and the methods actually employed to verify the identification in question.

Seventh, commissioners, magistrates and other judicial or quasi-judicial officials should be told in detail the possible hazards of Project SEARCH identifications, and should be encouraged to inquire in the course of their duties whether such data have been used and, if so, whether verification procedures have been completed. They should be asked to assume that any pretrial proceeding instituted on the basis of an unverified identification is fundamentally deficient. Police officers and prosecutors should be instructed to volunteer this information routinely, as part of their wider commitment to the integrity of the criminal justice process.

These precautions are not intended to invalidate any tentative identification information or responses for "on-the-scene" investigation and imminent arrest situations. Many innocent people may be immediately and intelligently cleared of suspicion, just as many guilty people may be held rather than summarily released, because of information derived from data obtained through the immediate nationwide record response of Project SEARCH.

At the same time, every effort should be made to reduce, through the application of relevant advanced technology, those circumstances in which Project SEARCH can provide only tentative identification to law enforcement officers and criminal justice agencies.

Secondary Uses of Data

The severity of the hazards created by any data system depends in large measure upon the purposes for which, and agencies by which, the system's information is employed. Constraints upon the system's collection and storage of data, no matter how rigorous, can never replace altogether a system of effective restrictions upon the uses to which those data are put. At the same time, such restrictions are often extraordinarily difficult to enforce. In this situation, for example, it must be anticipated that the data will frequently circulate widely through and outside the receiving agency. Police officers, prosecutors, detention officials, parole boards, clerical assistants, judicial administrators, public defenders, and many others may all be expected to demand copies of or access to the data. Licensing agencies, credit bureaus, the military

services, the communications media, private investigators, and others will make similar requests from outside the criminal justice community. Each of these groups will be likely to have informal constituencies with which it habitually exchanges information. Most of these secondary recipients will be only peripherally connected with the criminal justice process. The consequence is likely to be a network of very informal lines of communication, along which system's data will frequently flow. It must be acknowledged that no system of restrictions, however stringent, is likely to prevent all leakages. They are simply a fact of organizational life. Nonetheless, the committee believes that important steps may be taken that at least will reduce their frequency and seriousness to a minimum.

First, participating agencies should be instructed that no dissemination of system's data either within or outside the receiving agency is permissible except for purposes directly connected with the criminal justice process. A continuing program of employee training should be undertaken, in which the special constraints that are applicable to system's data are emphasized.

Second, as indicated earlier in this chapter, the committee recommends that data received through such a system be marked and readily identifiable as such. So far as administratively feasible, these data should not be intermingled with the receiving agency's ordinary files and documents.

Third, criminal justice agencies that obtain data from a receiving agency should be fully familiar with the system and with the special constraints that surround its data.

Fourth, receiving agencies should maintain, for a reasonable time, complete registers of the individuals and agencies to which the system's data are released. These registers should indicate the information released, the individual to whom it was released, and the date. It should be clearly understood that no further dissemination is permissible without specific, prior, and written consent from the receiving agency. If these restrictions are intentionally or repeatedly violated, the offending agency should be immediately denied further access to the system's data. The committee believes that these measures, together with those described in the subsection concerning access to the system, offer a realistic and constructive approach to these problems.

Research Uses

Another troublesome aspect of indirect access to the Project SEARCH system is in the area of research. Here we deal with the very legitimate interests of people who most often do not meet the criteria for direct access, yet granting indirect access to them would seem to be socially desirable.

When research into trends within the criminal justice field are conducted by Project SEARCH participants' own analysts, no special procedures are needed, other than to ensure that employees performing in this area abide by the privacy safeguards and rules. However, there has been strong interest, for the benefit of the criminal justice system, in making as much of this data as possible available to qualified social and behavioral science researchers.

If identifying numbers or names are needed in order to associate

information across time or conduct special studies, the researchers should indicate such needs and the actual search and link functions should be carried out by Project SEARCH personnel assigned to the project. The important point is that Project SEARCH can provide a means for mounting experimental programs of research within the purview of security and privacy constraints. There are political scientists, sociologists, lawyers, economists, and other specialists whose work in the criminal justice field could have a major impact in increasing our knowledge of both the causes of crime and effect of different commitments, and on probation policies and similar matters. Such programs of research may ultimately prove the most useful of all the consequences of such a system. Nonetheless, the committee strongly believes that all participating agencies should be obliged to take all reasonable steps to guarantee the privacy interests of the subjects of the records. It is convinced that these two competing interests may be satisfactorily accommodated by implementation of the following recommendations.

First, each participating agency and every proposed program of research should explicitly acknowledge a fundamental commitment to respect privacy interests in the conduct of research.

Second, no program of research utilizing individual records should be initiated unless an advisory council, or other appropriate representatives of the system, has fully investigated the proposed program, has been satisfied as to the professional qualifications of those involved, has been convinced that the proposal is justified by the public interest, and has approved the procedures it includes for the protection of individual privacy. Separate and explicit findings should be made as to each of these questions by the reviewing authorities.

Third, the identification of individual subjects should be divorced as fully and as effectually as possible from the data. Anonymity of the subjects should be actively sought in the design of the research project, and should be regarded as a fundamental characteristic of good research. Any research project not involving anonymity of the subjects should be examined with the greatest care. It should be assumed that any such project requires stringent supplementary protective measures, possibly including written prior consent from each subject whose file is to be opened.

Fourth, the research data should be shielded by a security system that, so far as reasonably possible, is fully comparable to that which ordinarily safeguards the system's data.

Fifth, any code or key that identifies individual subjects with any portion of the research data should be given special protection and should be destroyed as soon as reasonably possible.

Sixth, data obtained for one research purpose should not subsequently be used for any other research purpose without the prior, specific, and written consent of authorized representatives of the system. Such consent should be given only after reconsideration of all of the issues described above.

Seventh, each of these requirements, together with any supplementary requirements that may appear to be necessary in individual situations, should be included in any research contract or agreement. Appropriate nondisclosure forms should be required, and the system

should retain rights to monitor and, if necessary, terminate any program of research.

Finally, it must be understood by the relevant system representatives that these requirements should be extended or supplemented as needed to guarantee meaningful protection for the subjects' privacy interest. They are, in other words, intended to serve as an initial set of operating principles, and not as a final or comprehensive solution to the intricate problems of privacy and research.

VI. Organizational Structure, Controls, and Sanctions

It is important now to examine several more general questions of administrative policy. These may be conveniently divided into three groupings:

1. Questions of the proper legal and administrative relationships in the system, its participating agencies, and other public bodies.
2. Questions involving internal methods of control.
3. Questions involving the external remedies that should be provided those harmed by the system's activities.

Legal and Administrative Policies

Project SEARCH consists essentially of two parts: a central index, located during the demonstration in Michigan, and the various participating state agencies, each of which will prepare files for dissemination through the system and operate data terminals for the transmission and reception of data.

Both parts of Project SEARCH raise difficult questions of law and policy, but the committee believes that the system may best be structured along the following lines.

For reasons described earlier in this chapter, there should be a central computer within each state through which all data inquiries should necessarily pass. This central computer should be empowered to screen all data inquiries and to exclude those that appear inconsistent with the system's requirements. To facilitate this screening, every inquiry from a remote terminal should include prescribed minimal information concerning the requesting agency and the purposes of the inquiry.

This screening should be supplemented by, and cross-referenced against, a continuing program to monitor and supervise usage of the Project SEARCH system and its data within the state. Periodic usage reports should be required for each of the remote terminals.

Each state's Project SEARCH center's supervisory powers should include control over the position and number of remote terminals, as well as the character, number and sources of the data inquiries.

The committee believes that these obligations would be most effectively discharged if the central computer in each state were placed under the authority of a specific state agency. The agency should be adequately staffed with appropriately qualified professional personnel. It should be given, preferably by statute, ample authority to monitor and control usage of the system and its data within the state. This should include power to license remote terminals, to screen data inquiries, to require periodic activity reports, and to impose sanctions, including expulsion, on agencies and individuals that abuse the system.

An important organizational question relates to the actual placement and operation of the central index in any future system. A variety of devices might be employed for this purpose, each with its particular advantages and hazards. The index might, for example, be conducted on the basis of essentially informal understandings among the participating state agencies. This might be conveniently and easily created, but it is likely also to produce important legal and perhaps financial difficulties. The index might alternatively be placed under the authority of an existing or new federal agency. This method would have the possible advantage of encouraging continuing federal financing for the system. Third, the index might be conducted under the auspices of an interstate compact, joined by all of the participating states. This would give formal recognition to the states' primary responsibility for enforcement of the criminal laws, but it might, in addition, prove an awkward and inflexible arrangement that ultimately discouraged federal participation in the system.

Still another possibility might be a public corporation, chartered by the federal government. The committee does not believe that it should now offer recommendations as to these and other possibilities. Any final selection must await further clarification of the terms of any future system, including the relative financial responsibilities of the federal government and the participating states. Instead, the committee recommends simply that these and all other reasonable possibilities should be intensively examined to determine their relative advantages in light of the terms of any future system.

Internal Control

Whatever the legal structure ultimately selected for any future system, the committee believes that the following devices should be carefully considered for inclusion. First, there should be a permanent council of state representatives, supplemented by representatives of the relevant federal agencies and the general public. The public representatives should consist of a small number of distinguished private citizens, selected for their known interest in civil liberties and criminal justice.

This governing board should be given wide powers over the system including authority to:

- Monitor the activities of the participating state agencies.
- Adopt administrative rules and regulations for the system.
- Exercise sanctions over all agencies connected with the system.

The council should also have authority to delegate any and all of its powers to an executive committee. In addition, it should be supplemented by a small permanent staff, including a suitably qualified director, and such advisors and consultants as it finds necessary or appropriate.

Among its other activities, the council should conduct periodic investigations of the methods adopted by the participating states for the protection of privacy and security. It should from time to time formulate its findings into administrative standards for the entire system. It should exercise particular control over any proposed programs of research.

It should be clear that the committee envisions two layers of internal administrative controls for the system.

First, the individual state agencies should be generally responsible for the conduct of the system within their own jurisdictions.

Second, the national governing board and staff should monitor the activities of the several state agencies to insure proper cooperation and the full observance of national standards.

Both levels should be empowered to conduct investigatory hearings in which evidence would be taken, argument heard, and findings made. Both levels of administrative control should be empowered to impose prompt and appropriate sanctions upon any agency that has abused the system or its data.

The sanctions at both levels could involve suspension or expulsion of agencies from the system. However, at the state level, in cases of individual offenders, there should be a whole range of employment sanctions, including discharge.

Further, the committee believes that administrative sanctions should be supplemented by the imposition of criminal penalties upon those who willfully misuse the system or its data. These penalties ought to include the possibility of terms of imprisonment as well as fines. They might be created by federal or state statutes, or some combination of the two, but the committee recommends that the system should draft, and each participating state should immediately adopt, a uniform act for the protection and control of system data. This model statute should include these criminal penalties, the civil rights of action described below, and any exemptions that may be necessary from state licensing and freedom of information statutes. These last issues are discussed in earlier sections of this chapter.

External Remedies

It is necessary next to examine the various remedies that should be provided those who are injured by the system's activities. We have already described the rights of access, notice, and challenge which we would have the system guarantee to every individual. The committee does not, however, believe that these rights, important as they certainly are, should be thought adequate.

The legal history of this country consists in large measure of warnings that administrative remedies are in themselves insufficient guarantees of individual interests. More narrowly, it should be clear that any future system will win the confidence of the general public only if it first provides tangible evidence of genuine concern for the rights of those about whom it will collect information. A meaningful system of judicial remedies would provide such evidence. Two sets of remedies should be considered: First, the administrative rights of notice, access, challenge, and review should be made judicially enforceable by statutory authorization of a prerogative writ, on the order of mandamus and habeas corpus. This in itself will add nothing to the burdens or inconveniences placed upon the data system by these rights. It merely provides persuasive testimony that these rights are seriously intended and that they may, if necessary, be guaranteed by the courts.

Second, statutory authorization should be given for broadened civil rights of action in cases in which inaccurate, incomplete, or misused data cause injury to the data's subjects.

As the situation now stands, private citizens in most states are given

civil causes of action in cases of defamation, invasions of privacy, and breaches of confidentiality. These rights of action are, however, often of little practical value because of various exceptions and limitations. The pressures and situations that shaped these restrictions have little relevance to the issues that now concern us.

The committee, therefore, recommends the creation by statute of supplementary civil rights of action, under which individuals could recover actual damages suffered as a consequence of negligent or willful misconduct by the data system or its employees.

These rights would run separately, but not cumulatively, against the system and its participating agencies. They should be included in a model statute drafted by the system and adopted in each of its participating states.

Finally, attention should be given to the various proposals that data systems should supplement their internal controls by the use of ombudsmen or independent boards of inquiry. The committee has examined these suggestions closely, but has concluded that its recommendation for public representatives on the national council is in this situation more satisfactory. The committee anticipates that this will guarantee the same independence of view without the same administrative inconveniences.

Nonetheless, the committee recommends that these additional protective devices should periodically be reconsidered by the council and staff of any future system. Perhaps, these devices might later be used on an experimental basis in selected states. The point that warrants reemphasis here is that individual privacy interests can be effectively protected only if they receive serious and sympathetic attention from every participating agency throughout the life of the system. This is, as we observed earlier, the committee's first and most fundamental recommendation.

Chapter 4
System Security

The previous chapter has described a broad range of considerations relating to the design and operation of a total computerized criminal history system, from the viewpoint of providing guidelines protecting individual privacy. There are two aspects of the entire security and privacy question that remain to be addressed.

First, while it is appropriate to discuss the privacy considerations with respect to the total operational system (hardware, software, operators, and users), the actual implementation of many of these guidelines will ultimately be carried out by the agency that is chosen to operate each state system. These system operators will be assigned the responsibility, then, of providing the actual detailed procedures that accomplish the recommendations of Chapter 3. It is, therefore, appropriate to view the considerations of Chapter 3 in terms of how they affect actual system operation, and thereby provide guidance for system operators in preparing the necessary procedures.

Second, there are a second set of considerations interrelated with the privacy issues that concern the system operators. These relate to the protection which must be given to the system to preclude damage or loss that will impair the operation of the system. Obviously, a heavy reliance on the system requires that it be protected from accidental or intentional damage or alteration. These concerns also imply that the system operators have to develop appropriate procedures.

When the privacy issues are viewed from the perspective of the system operator, the resulting procedures overlap those that would be developed for the protection of the operating system. It is, therefore, useful to consider the combination of these two aspects in terms of system security.

System security, then, is the ability to restrict the availability of specific information to authorized individuals, and the ability to physically protect all parts of the system, including both data and the system that processes the data, from any form of hazard that might endanger its integrity or reliability.

This chapter is organized under seven major headings representing statements of security/privacy agreed to by the Project Group representing the states participating in Project SEARCH. These policy statements represent the commitment of the participating states to system security as an integral part of criminal justice information system design and operation. They are expected to remain relatively constant over time, and to be useful both in the conduct of the feasibility demonstration being conducted under Project SEARCH and in the design and operation of future national criminal history information systems.

Immediately following each major policy statement, procedures consistent with that policy are presented. These procedures are intended to be illustrative of the types of activities which states would undertake in implementing the policy statements. It is recognized that the specific

procedures to be implemented in a given state, and the timing of implementation, will vary widely, depending on the statutory authority of the agency operating the criminal justice information system, state statutes regarding security and privacy, the equipment and software configuration of the system, the numbers and types of system users within the state, and other variables. Because of these variations, and because the security and privacy committee realizes that it is impractical to attempt to specify detailed operating procedures which can and will be adopted by every agency, the guidelines presented here are explicitly limited to illustrations. Although it may be possible in the development of a future system to identify mutually acceptable procedures, a much broader involvement of the participants will be necessary to reach agreements that will actually be implemented. At the present time, some of the procedures listed in this chapter may be inappropriate in some participating states, whereas procedures not discussed in this chapter may be very desirable or already implemented in other states. The important point is that participating states concur in the policy statements, and recognize a requirement to translate these policy statements into day-to-day performance.

In order to be effective, procedures must be brief, unambiguous, and directed toward action (that is, they should require some actions, allow others, and forbid still others). Procedures must be available to all authorized users of the system whose actions are affected by them and they must be made an integral part of job training and performance evaluation. Whereas policy statements are expected to remain valid over extended periods of time, procedures must be continually evaluated in the light of changes in the state of technology, system configuration, and external security risks.

Policy Statement: *The input, modification, cancellation, or retrieval of information from the system will be limited to authorized agency terminals.*

A procedure consistent with this policy would require the identification of individual terminals using a method not requiring operator intervention (e.g., terminal "hardware").

For systems on which terminals are shared by authorized agencies and unauthorized agencies, procedures to implement passwords, scheduling, operator identification, or off-line initiation of system actuation (e.g., by telephone call) are consistent with this policy statement.

For systems in which some agencies are authorized limited system access (e.g., inquiry only terminals) consistent procedures would define levels of access to the system in terms of types of information elements and records which can be input, modified, cancelled, or retrieved by each and every agency, coupled with system software provisions to insure that only those system transactions authorized can be undertaken by each participating agency.

Procedures to insure that the telecommunications facilities of the system are adequately protected against eavesdropping, tapping, insertion of false messages, and so forth are within the scope of this policy statement. If the system is implemented on a computer system not entirely dedicated to criminal justice applications, procedures to protect or to prohibit access to the data base by unauthorized agencies during time-sharing, multi-programming, or other uses of the processor should be implemented.

Policy Statement: *Disclosure of information from the system through terminals will be limited to authorized final users.*

Procedures for the training and education of terminal operators and user personnel within agencies fall within the scope of this policy statement. Such procedures include the mandatory posting of rules and statutes applicable to use of the information, establishment of a mandatory training program as a condition of system participation, and refresher training in security requirements.

Procedures to assure the prompt and active prosecution of persons accused of unauthorized information use, and for cancellation of system services to agencies which violate system security would also fall within the scope of this policy statement.

Procedures to require the establishment, maintenance, and review of system usage logs for the identification and documentation of system security violations would support this policy statement.

Procedural requirements for physical security standards at terminal locations regarding physical access to the terminal by staff, maintenance personnel, and visitors, and for the disposal of printouts and other system byproducts will support this limitation of information access.

Procedures to assure the limited distribution of Operating Manuals and other information required for access to the system will support this policy. Procedures requiring dedicated communications facilities and lines assist in implementing this policy.

Policy Statement: *Information in the system will be protected against unauthorized access in the computer center.*

Procedures to assure the secure and orderly destruction of page printer and paper tape output of the information system provide partial implementation of this policy. Similarly, procedures for the erasure of magnetic tapes and discs prior to transfer out of the computer center or reuse in portions of the center not devoted to criminal justice information processing are appropriate implementations of this policy.

Procedures providing for the physical security of the computer center, including procedures for escorting of visitors, maintenance personnel, and equipment vendor representatives will reduce the risk of unauthorized access.

General software requirements for the erasure and clearance of core, buffers, mass storage, and peripheral equipment as an integral part of all programs dealing with the processing and retrieval of criminal justice information lend credence to the policy statement.

Procedures for the limitation of the numbers and the qualifications of computer center personnel authorized to have direct access to the information in the computerized system through the system control terminal, and providing for the logging of system transactions through the control terminal represents an important portion of the policy implementation plan.

Policy Statement: *Information in the system will be protected against unauthorized alteration.*

Procedures which require the installation, checkout, and regular review of file protection software is an appropriate response to this policy statement. Care must be taken that the file protection software concept

used really protects against accidental or intentional alteration of individual files under all operating circumstances.

Procedures assuring that the criteria for purging of individual information elements or records from the file are clearly and concisely stated, published, and made available to all authorized users of the system should be developed. A procedure requiring the logging of all record alteration transactions of the system and periodic review of those logs can be implemented.

A procedure of special review of information purging software should be carried out, to determine if the user should be authorized to purge records without manual intervention at the computer site.

Policy Statement: *Information in the system will be protected against loss.*

Procedures for the protection of the computer facility and files against fire and vandalism should be instituted, to include specific requirements of site preparation and configuration to assure that strong countermeasures against fire and vandalism can be mobilized, and to minimize the probability that total loss of data will occur.

Procedures which establish library storage of system information should be instituted, with special consideration for the environmental control to allow long-term storage of data without degradation, proper internal and external labeling to assure ease of retrieving information from the library, and proper physical protection of the library facilities to protect against (and detect attempts at) access by unauthorized persons.

Procedures should be instituted to assure special protection of information in the system during critical periods of system configuration change such as file reformatting, reprogramming, changes in information retrieval/modification programs, etc.

Procedures to limit the total number of persons who have "complete" access to the system, through implementation of privileged instruction sets or limitations on the capabilities of individual input/output devices are within the scope of this policy statement.

A procedure for the protection of the computer center and telecommunications lines against tapping, eavesdropping, and imitative deception techniques should be instituted; the procedure should detail responsibility for concern about these danger areas during system design, operation, and modification phases.

Since information unavailable at the time of need is essentially "lost", the provision of facility duplexing, gradual failure modes, and other equipment and procedures designed to maximize system availability support this policy. Procedures requiring the storage of duplicate files, programs, and documentation separate from the computer center similarly support this policy.

Policy Statement: *Information in the system will be protected against unauthorized use.*

Procedures to identify specifically those uses to which the information base can be put should be instituted. These procedures will include definitions of those uses which fall within the direct functional responsibilities of the criminal justice information system, those statutorally mandated, those allowed uses within the discretion of the information system management, and uses specifically forbidden by statute or ad-

ministrative decision. Included should be both operational and research uses of the data, by both governmental and private agencies, as described in Chapter 3.

Procedures for the editing of data before turning it over to researchers, and for the training and education of those users in security should be explicitly stated in written procedures.

Procedures to establish records of such secondary uses of the data, containing both the authorization under which the use was obtained and the specific information to which the user had access are within the scope of this policy statement.

Procedures for the authorization of computer program preparation, coding, debugging, test, and use on the system including standards of documentation required and specific check for security adherence are proper partial implementations of this policy statement.

Policy Statement: *System security is a line responsibility equal in importance to system performance.*

An appropriate implementation of this policy statement would include procedures to insure that appropriate consideration is given to security risk at the point of hiring, performance review, and promotion. Implementation may include required background investigations, setting of personnel standards concerning criminal history of persons with access to the system (possibly equivalent to police officer standards), probationary employment periods, and continuing activities to investigate the risk potential of system employees, vendors, maintenance personnel, etc. In the case of computer centers not entirely under the management control of criminal justice agencies, these provisions may extend to government employees of other agencies.

There should be procedures of periodic management audit of security procedures for the system, to insure that existing procedures are adequately stated, published, and adhered to. In addition, the audit should review all phases of security to determine the adequacy of current procedures to the current security risks, and to develop additional procedures where required.

Procedures calling for external audit of security adequacy either periodically (e.g., every four years) or on special occasions (e.g., after a major security violation) would support this policy statement.

Appendix A
Code of Ethics

Project SEARCH participants believe that a nationwide capability for quick access to offender criminal histories is essential for effective law enforcement and administration of criminal justice.

It is recognized, however, that the extraordinary increase in accessibility and responsiveness associated with the use of computer-based information systems may increase the possibility of unauthorized disclosure or misuse of the data in other than legitimate law enforcement and criminal justice functions. Therefore, in order to provide reasonable protection of individual privacy and to secure the data maintained in the System, the participants in Project SEARCH pledge to observe the following:

Article I. Limitations of the System

SECTION 1. *Limited area of government.* The participants should limit the area of concern to criminal justice as a matter of government function.

SECTION 2. *Limited category of users.* The participants should limit access to the System to criminal justice agencies who would assume responsibility for the legitimate criminal justice use of System data and provide penalties for improper disclosure. Rules governing access should be definite and subject to public scrutiny.

SECTION 3. *Limited functions.*

A. The participants should limit the role of the Central Index to an information service only.

B. The participants should limit the System, at the national level, to an index or directory role rather than a registry function.

SECTION 4. *Limited information.*

A. The participants should limit System records to certain subjects —those for whom arrest fingerprints have been recorded. The recording of data about an individual should be initiated only upon the report of a crime and the commencement of criminal justice system proceedings.

B. The participants should limit data collection to only that which is relevant for the criminal justice process. Thus, data about individuals such as contained in census, tax, election, unemployment insurance, and similar files should not be collected or accessed through the System.

C. The participants should specifically exclude from the System all unverified information such as informant-supplied data or intelligence data.

Article II. Integrity of Information

SECTION 1. *Assurance of individual privacy.* The participants should make a continuous effort to refine every step of the criminal justice information system provided by SEARCH to assure that the most sophisticated measures are employed and the most perceptive judgments are made in the development and operation of the System to

optimize the protection of individual privacy.

SECTION 2. *Collection and maintenance of data.*

A. The participants should be greatly concerned with the completeness and accuracy of the information in the System. Regular auditing of the data bank should be undertaken to assure the reliability of stored data.

B. The participants should establish criteria for re-evaluation of the data contained in the System and for purging where deemed appropriate.

C. The participants should provide measures for purging from the Central Index the computerized file of the record of first offenders where criminal proceedings have resulted in a determination in favor of such persons.

D. The participants should encourage the provision of procedures for an individual to learn the contents of the arrest record kept about him and for the correction of inaccuracies or prejudicial omissions in a person's arrest record.

SECTION 3. *Dissemination of data.*

A. The participants should develop a classification sub-system to assure that sensitive data is provided premium security and that all data is accorded appropriate protection. Data should be disseminated to criminal justice agencies on a "need-to-know" basis.

B. The participants should make provisions in appropriate cases to limit the derogatory impact of arrest records by providing meaningful descriptions of the nature of a person's criminal act so that false conclusions concerning the character of the individual are avoided.

C. The participants should employ a high level of computer, legal, physical, information, communications, and personnel security methods to reduce the possibility of breaching the security of the System.

SECTION 4. *Advisory committee.* The participants should establish an advisory committee to provide policy direction for the System and to entertain complaints about alleged intrusions on individual privacy.

Article III. Use of Data Base for Research

SECTION 1. *Commitment to privacy.* Where research is conducted as an activity of the System or utilizing data contained in the System Data Bank, the participants should recognize and affirm the claim to private personality and have a positive commitment to respect it.

SECTION 2. *Safeguarding anonymity.*

A. In the conduct of research, participants should divorce the identification of the individual as fully and as effectively as possible from the data furnished and preserve anonymity by aggregating, coding, and other appropriate measures.

B. Participants should safeguard research data in every feasible and reasonable way, and destroy the identification of the individual with any portion of the data as soon as possible, consistent with the research objectives.

Appendix B
Biographical Data
Security and Privacy Committee

DR. ROBERT R. J. GALLATI, *Chairman*

Dr. Gallati is currently the Director of the New York State Identification and Intelligence System, a computer-based information system serving the criminal justice community of the State. Before his appointment to this position in 1964, Dr. Gallati served with the New York City Police Department for 27 years.

Dr. Gallati received the Doctoral degree in Jurisprudence, Summa Cum Laude, at Brooklyn Law School in 1957 and is presently a candidate for the degree of Doctor of Public Administration at NYU. He is a member of the Bar of New York and admitted to practice in the U.S. Supreme Court and a number of other jurisdictions. As a member of the International Association of Chiefs of Police, he has served the Association in a number of capacities.

He is the author of several published articles on Police Administration and Training and coauthor of *Introduction to Law Enforcement.*

C. J. BEDDOME

Captain Beddome is Commander of the Data Processing Section of the Arizona Department of Public Safety. He has been associated with the Arizona Highway Patrol since 1954. After graduating from Northwestern University Traffic Institute in 1962, he was assigned command of the Records Bureau until 1968.

Captain Beddome was among those who set the standards and procedures for the FBI's NCIC system, and has assisted in the development of numerous police record-keeping and data processing systems.

GEORGE E. HALL

Mr. Hall is the Director of the National Criminal Justice Statistics Center within the Law Enforcement Assistance Administration. He was formerly with the United States Bureau of the Census.

In 1969, he received the United States Department of Commerce Silver Medal for Outstanding Federal Service in the development of statistical programs. He received a B.A. in Economics from Howard University.

H. W. McFARLING

Chief McFarling has, since October 1967, been head of the Data Processing Division of the Texas Department of Public Safety. Immediately prior to this appointment, he served as chairman of the committee studying the feasibility of a comprehensive computer system for the Department of Public Safety. He has served with the department since 1938, and since 1957, has specialized in program development, inspection, and planning.

Chief McFarling has taught in the Texas Municipal Police School and the Department of Public Safety's Recruit Training Schools for a number of years.

EMERY BARRETTE

Mr. Barrette is the Executive Director of the Minnesota Governor's Commission on Crime Prevention and Control. He is a member of the St. Paul Board of Education and is an ordained United Methodist minister.

He was a member of the Minnesota House of Representatives (1967–69) and authored considerable criminal justice legislation. He formerly served as a chaplain in the county workhouse and jail, the juvenile court and city police department.

He was named one of Ten Outstanding Young Men of Minnesota in 1965 and received the Liberty Bell Award and Service to Freedom Award from the Ramsey County and

Minnesota Bar Associations in 1966. He received a B.A. from Hamline University and a B.D. from Drew University.

DAVID R. WEINSTEIN

Mr. Weinstein is the Executive Director, State of Connecticut Planning Committee on Criminal Administration. He earned a B.A. (magna cum laude) from Yale University in 1959 and an L.L.B. (cum laude) from Harvard Law School in 1962.

CONSULTANTS

CHARLES LISTER

Professor Lister is currently an Associate Professor at the Yale Law School. His major teaching and research activities center on constitutional law and history, with particular emphasis on the emerging constitutional right of privacy.

Mr. Lister graduated from Harvard in 1960, magna cum laude, and attended Oxford University as a Rhodes Scholar receiving a graduate degree in law in 1963.

Immediately prior to accepting a position at Yale, Professor Lister served as law clerk to Mr. Justice John M. Harlan of the U.S. Supreme Court. He is a member of the Bar of the District of Columbia.

JEROME LOBEL

Mr. Lobel is currently Regional Supervisor of Management Services for Ernst & Ernst in Phoenix, Arizona. He has worked extensively in Arizona and California in the development of data processing systems.

Mr. Lobel received his B.S. and M.B.A. from UCLA and has had over 18 years of experience in a variety of data processing and management assignments.

He has particular expertise in computer security problems. One of his major assignment areas in recent years has been the comprehensive evaluation of controls in computer installations of numerous Ernst & Ernst clients.

Appendix C
Glossary of Terms

Application Program

Computer programs that perform user-oriented functions or solve user problems.

Auxiliary Storage

Devices that may be connected to a computer to hold data for subsequent processing. Also called secondary storage. Examples include drums, disk drives, magnetic tape transports, and other peripheral devices.

Batch Processing

The processing of data in a sequential or serial fashion. The data consists of similar items or transactions that have been specially sorted and batched for processing purposes.

Buffer

Auxiliary data storage outside of main memory designed to hold data temporarily and to compensate for speed differences between slower electromechanical input/output devices and the speed of the computer's central processor.

Central Processor Unit (CPU)

That part of a computer system that controls instruction execution and internal memory. It normally contains the arithmetic unit and special registers.

Core

The internal memory of a computer consisting of tiny, doughnut-shaped components about the size of a pinhead. Cores are made from a special ferromagnetic, ceramic material. Each core is capable of storing in magnetized form one bit of data.

Coresident Program

The condition where more than one computer program is allowed to reside in and share the internal memory of a computer.

Criminal Case History

The record(s) of an individual resulting from each formal stage of the criminal justice process.

Criminal Justice System

That part of governmental jurisdiction that encompasses the broad functions of police, prosecution, criminal courts, probation, correctional institutions and parole.

Data Bank

A centralized collection of information which may take any number of forms, among them:

Autonomous. Wholly for statistical studies and services; no regulatory/control functions.

Independent. Information coordination confined to one subject area; not part of any line operations.

Interagency Administrative. Data collection and management for general administration at a particular layer of government.

Agency. A computer system within one agency to collect and use data to aid in decision-making.

Mixed Public/Private. Combined effort of government and private agencies; established under a private trust agreement.

Data Track

A sequence of binary cells arranged in a way that permits serial reading or writing on some surface. It is the part of a moving storage media such as a tape, disk, or drum that is accessible to a particular read/write station.

Degaussing

A protective measure that involves overwriting or re-recording on a magnetic surface in such a way as to completely erase the original data.

Digital Computer

A device capable of performing a series of internally stored instructions such as certain arithmetic or logical operations.

Direct Access Devices

Devices that may be connected to a computer (directly or at a remote location), and are capable of accessing on-line computer files and other system components. A terminal is a typical direct access device.

Due Process

The legal rights of an individual to know about, explain and challenge any information used to make official judgments about him in the public sphere of government action.

Electromagnetic Radiation

The wave-lengths or frequencies produced by a source of electric current.

External Labeling

The physical labeling of removable storage media.

File Protect

A protective feature designed to prevent accidental overwriting of data on magnetic media already containing other live or vital data. An example would be a removable file protect ring.

Forgiveness Principle

The philosophy which results in the removal from an active file (or erasure) of dated information that is no longer directly relevant to decisions to be made about an individual.

Hardware

Any physical part of a computer-oriented equipment configuration.

Individual Privacy

The legal and moral right to be safeguarded against a personal intrusion as a result of having sensitive personal information fall into the possession of an unauthorized receiver.

Information Compromise

To intentionally or accidentally expose or surrender information to an unauthorized receiver.

Instruction

A coded program step that directs a computer to perform a particular operation.

Integrity

The assurance that data in a system is protected against compromise or contamination.

Intelligence

The result of the collection, correlation, and analysis of data from a wide variety of sources: identification, criminal histories, unverified reports, covert sources, etc.

Internal Labeling

The magnetic recording of file identification and contents at the beginning and end of each tape or disk, etc.

Law Enforcement Assistance Administration (LEAA)

The agency within the Department of Justice established to administer the Omnibus Crime Control and Safe Streets Act of 1968.

Memory

A device which can hold information. A primary example would be core memory in a computer.

Memory Protect

A feature that provides protection to programs, data, and operating systems that may be residing in the memory of a computer.

Modem

An integral part of a data communications system used to interface a carrier to a line terminal.

Multiprocessing

The combined use of two or more connected computers, which share each other's resources such as input-output capabilities and peripheral devices.

Multiprogramming

The ability to run two or more programs in the internal memory of a computer at the same time.

National Crime Information Center (NCIC)

A computerized index and communications network linking law enforcement agencies throughout the United States with the FBI.

Need-to-Know

The specification of what kind(s) of information is to be made available to a qualified user of a data system.

On-Line Files

Files held in some auxiliary storage devices that are directly connected to and accessible to a computer.

Operating System

The programming system inserted into a computer to control and simplify certain basic functions such as input-output procedures, data conversion, tests, and other system subroutines (programs).

Overwriting

Changing existing magnetically recorded data to some other data by "writing-over" or re-recording on the same surface.

Privacy

The claim by individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

Privileged Instructions

Special computer instructions designed to reduce the misuse of one program input-output device by another program.

Program

The detailed instructions that tell the computer how to proceed in solving a problem.

Project SEARCH

Project SEARCH (an acronym for System for Electronic Analysis and Retrieval of Criminal Histories). A project to demonstrate the capabilities of interstate exchange of criminal history data and statistical retrieval.

Public Record

Data recorded by public officers in consequence of public duties, at the conclusion of relatively formal and often public proceedings.

Purging

A system for the orderly review of a file's content to remove inactive or low-value data.

Right-to-Know

Specification, by statute or administrative rule, as to who shall have access to an information system.

Security

The protection of information in storage and transit from unauthorized access or tampering.

Sensitivity (Data)

Anticipate consequences of disclosure or modification of data.

Software

Computer programs and all supporting documentation such as logic diagrams and instruction or program listings.

Storage Media

Removable or non-removable devices or components that contain machine readable data. Removable storage media may be referred to as external storage since that data can be completely removed from the computer. Examples include disk packs, magnetic tape reels, punched cards, and paper tape.

System Security

The ability to restrict the availability of specific information to authorized individuals, and the ability to physically protect all parts of the system, including both the data and the system that processes the data from any form of hazard that might endanger its integrity or reliability.

System Supervisor

A special control program normally part of an operating system. A program designed to control loading and relocation of other programs.

Terminal

An input-output device that may be connected to the computer directly or at some remote (distant) location.

Time-Sharing

The use of a computer by two or more users (located at the computer or at remote terminals) in such a way as to appear to each user that he is the sole occupant of the system.

Unauthorized Disclosure

The release of information to those not qualified to receive it.

Appendix D
Selected Bibliography

I. BOOKS

Allen, Layman E., and Caldwell, M. E. *Communications Science and Law.* New York: Bobbs Merrill, 1965.

Barker, Lucius J., and Barker, Twiley W. *Freedoms, Courts, Politics: Studies in Civil Liberties.* Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1965.

Brenton, Myron. *The Privacy Invaders.* New York: Coward-McCann, Inc., 1964.

Burck, Gilbert, *et al. The Computer Age.* New York: Harper and Row, Publishers, 1965.

Cipes, Robert M. *The Crime War.* New York: World Publishing, 1968.

Cushman, Robert F. *Civil Liberties in The United States.* Ithaca, N.Y.: Cornell University Press, 1966.

Gregory, Robert H., and Van Horn, Richard L. *Automatic Data Processing Systems: Principles and Procedures.* 2nd edition. Belmont, Calif.: Wadsworth Publishing Co., 1963.

Gross, Hyman. *Privacy—Its Legal Protection.* New York: Oceana Publications, Inc., 1964.

Hattery, Lowell H. *Executive Control and Data Processing.* Washington, D.C.: Anderson Kramer Associates, 1959.

Hearle, Edward and Mason, Raymond J. *A Data Processing System for State and Local Governments.* Englewood Cliffs, N.J.: Prentice-Hall, 1963.

Hofstader, Samuel H. *The Development of the Right of Privacy in New York.* New York: The Grosby Press, 1954.

Johnson, Richard A., and Kast, Fremont E. *The Theory and Management of Systems.* New York: McGraw-Hill Book Company, Inc., 1963.

Jones, Edgar A. (ed.). *Law and Electronics: The Challenge of a New Era.* Albany: Matthew Bender, 1962.

Kozmetsky, George, and Kircher, Paul. *Electronic Computers and Management Control.* New York: McGraw-Hill Book Company, Inc., 1956.

Long, E. V. *The Intruders: The Invasion of Privacy by Government and Industry.* Frederick A. Praeger, N.Y. 1967.

Orwell, George. *1984.* New York: Harcourt Brace and World, Inc., 1949.

Packard, Vance. *The Naked Society.* New York: David McKay, 1964.

Rubinoff, Morris. *Toward a National Information System.* Washington, D.C.: Spartan Books, 1965.

Shils, Edward. "Social Inquiry and the Autonomy of the Individual," in Lerner, Daniel (ed.). *The Human Meaning of the Social Sciences.* Cleveland: World Publishing Co., 1959.

Thomas, Shirley. *Computers.* New York: Holt, Rinehart, and Winston, 1965.

Tomeski, Edward A., Wescott, Richard W., and Covington, Mary (eds.). *The Clarification, Unification and Integration of Information Storage and Retrieval.* New York: Management Dynamics, 1961.

Trebach, Arnold. *The Rationing of Justice.* New Brunswick, N.J.: Rutgers University Press, 1964.

Westin, Alan F. *Privacy and Freedom.* Atheneum, N.Y. 1967.

II. PERIODICALS

Bates, Alan. "Privacy—A Useful Concept?" 42 *Social Forces* 1964.

Bergamini, David. "Government by Computers." *The Reporter,* XXV, No. 3 (August 17, 1961), 21–28.

Bigelow, R. P. "Automation and the Law," *Boston Bar Journal* VI (September, 1962), 31–33.

Bigelow, Robert P. "Legal and Security Issues Posed by Computer Utilities." *Harvard Business Review,* Vol. 45, No. 5, Sept.–Oct. 1967.

Bisco, Ralph L. "Social Science Data Archives: A Review of Developments," *American Political Science Review,* LX (March 1966), 93–109.

Boehm, George A. W. "The Next Generation of Computers," *Fortune,* LX (March 1959), 132–135.

Buckley, J. L. "Computers, Automation, and Security." *Law and Order,* March 1965.

Buckley, J. L. "The Future of Computers in Security and Law Enforcement." *Law and Order,* August 1965, Pt. 1 and 2.

Campbell, Alan and Woods, Alan. "Computers and Freedom". *Law and Computer Technology,* June 1969.

"Computers: A Question of Privacy". *Electronics,* February 6, 1967, 36–38.

Computerworld:

—"Data Files Greatly Threaten Individual Privacy", December 17, 1969.

—"Congress Warned on Two Proposed Giant Data Banks." December 31, 1969.

—"Computer May Become 'Tool of Repression' ", December 24, 1969.

—"Writ of 'Habeas Data' Advocated by Westin", January 21, 1970.

Davis, Frederick. "What Do We Mean by 'Right to Privacy'," *South Dakota Law Review,* IV (Spring 1959), 1–24.

Ervin, Sam J. "The Computer and Individual Privacy." *Vital Speeches of the Day,* (May 1, 1967), 421.

Gallati, Robert R. J. "Criminal Justice Systems and the Right to Privacy." *Public Automation,* (July, 1967).

Heckscher, August. "The Invasion of Privacy: The Reshaping of Privacy," *American Scholar,* 13 (1959).

"Invasion of Privacy," *University of Pittsburgh Law Review,* XIX (Fall, 1957), 98–111.

Karst, K. L. "The Files: Legal Controls Over the Accuracy and Accessibility of Stored Personal Data," *Law and Contemporary Problems,* Vol. 31 (Spring, 1966).

King, D. B. "Electronic Surveillance and Constitutional Rights: Some Recent Developments and Observations," *George Washington Law Review,* XXX (October, 1964), 240–269.

Lasswell, H. D. "The Threat to Privacy," in R. M. MacIver (ed.) *The Conflict of Loyalties,* (1952).

Lear, John. "Whither Personal Privacy," *Saturday Review,* July 23, 1966.

McCarthy, John. "Information," *Scientific American,* CCXV, No. 3 (September, 1966), 65–72.

Meldman, Jeffrey A. "Centralized Information Systems and the Legal Right to Privacy," *Marquette Law Review,* Vol. 52, No. 3 (Fall, 1969).

Michael, D. N. "Speculations on Relation of Computer to Individual Freedom and the Right to Privacy," *George Washington Law Review,* XXX (October, 1964), 270–286.

Miller, Arthur R. "The National Data Center and Personal Privacy," *The Atlantic,* Vol. 220, No. 5 (November, 1967).

Packard, Vance. "Don't Tell It to the Computers," *NY Times Magazine,* January 8, 1967.

Price, Dennis G., and Mulvihill, Dennis E. "The Present and Future Use of Computers in State Government," *Public Administration Review,* XXV, No. 2 (June, 1965), 142–150.

"Privacy: Debate Will Rage and Confuse the Issues, But a National Data Center Will Become Reality." *Business Automation,* January, 1970.

"Privacy," *Law and Contemporary Problems,* XXXI, No. 2 (Spring, 1966).

Prosser, William. "Privacy," *California Law Review*, XLVIII No. 3 (August, 1960), 383–423.

Revere, Richard. "The Invasion of Privacy: Technology and the Claims of Community," 27 *American Scholar*, 416 (1958).

Ruebhausen, Oscar M., and Brim, Jr., Orville, G. "Privacy and Behavioral Research," *Columbia Law Review*, LXV (November, 1965), 1184–1211.

"Science, Technology and the Law." *Saturday Review*, Vol. LI., No. 31, (August 3, 1968), pp 39–52.

Shils, Edward A. "Privacy: Its Constitution and Vicissitudes," 31 *Law and Contemporary Problems*, 281 (Spring, 1966).

Stone, J. "Man and Machine in the Search for Justice," *Stanford Law Review*, XVI (May, 1964), 515–560.

"System Development for Regional, State, and Local Government," *System Development Corporation Magazine*, VII, No. 10 (October, 1965), 1–27.

Warren, Samuel D., and Brandeis, Louis D. "The Right to Privacy," *Harvard Law Review*, IV, No. 5 (February, 1890), 193–220.

Weeks, James. K. "Comparative Law of Privacy," *Clev. Mar. Law Review*, XXII (September, 1963), 484–502.

Westin, Alan F. "Science, Privacy, and Freedom: Issues and Proposals for the 1970's" Part I: "The Current Impact of Surveillance on Privacy," *Columbia Law Review*, LXVI, No. 6 (June, 1966), 1004–1048. Part II: "Balancing the Conflicting Demands of Privacy, Disclosure, and Surveillance," *Columbia Law Review*, LXVI, No. 7 (November, 1966), 1205–1253.

Westin, Alan F. "New Laws Will Protect Your Privacy," *Think*, May/June, 1969.

III. PUBLICATIONS OF THE GOVERNMENT, LEARNED SOCIETIES, AND OTHER ORGANIZATIONS

American Federation of Information Processing Societies. *Conference Proceedings*, 1967 Spring Joint Computer Conference. Washington, D.C.: Thompson Books, 1967.

American Management Association. *Computer-Based Management for Information and Control.* New York: American Management Association, 1963.

American Society for Public Administration. *Automation in Government*, 1963. Washington, D.C.: American Society for Public Administration, 1963.

Armer, Paul. "Social Implications of the Computer Utility." RAND Corp., Santa Monica, Calif. (Aug. 1967).

Baran, Paul. "The Coming Computer Utility Laissez-Faire, Licensing or Regulation?" (April, 1967), RAND Corp., Santa Monica.

Bingham, H. W. *Security Techniques for EDP of Multilevel Classified Information.* New York: Rome Air Development Center, Air Force Systems Command, Griffis Air Force Base, 1965.

Brictson, R. C. "Computers and Privacy—Implications of a Management Tool." SDC, (March 14, 1968).

Burroughs B5500 File Security System. *New York State Identification and Intelligence System.* Document prepared for computer security. "Burroughs B5500 File Security System."

The Challenge of Crime in a Free Society. Report of President's Commission on Law Enforcement and Administration of Justice. (February, 1967).

Comber, Edward V. "Management of Confidential Information." System Dynamics, Inc., Oakland. Submitted to Fall Joint Computer Conference, 1969.

Computer and Invasion of Privacy. Hearings before a Subcommittee of the Committee on Government Operations, HR, 89th Congress, 2nd Session, (July 26–28, 1966).

Council of State Governments and Public Administration Service. *Automated Data Processing State Governments.* Chicago: Public Administration Service, 1965.

Cuadra, C., Isaacs, H. H., Neeland, F., and Wallace, E. M. *An Information Center for Law Enforcement.* A report prepared by System Development Corporation, Santa Monica, California. 1964.

Dennis, Robert L. *Security in the Computer Environment.* A summary of the Quarterly Seminar, Research Security Administrators, June 17, 1965. Santa Monica, California: System Development Corporation, 1966.

Fanwick, Charles. "Maintaining Privacy of Computerized Data." System Development Corporation, 1966.

"Federal Data Centers—Present and Proposed". *Computer Privacy.* Hearings before the Subcommittee on Administrative Practice and Procedure, Committee on the Judiciary, U.S. Senate, 90th Congress, 1st Session, March 14–15, 1967.

IBM Corporation. "Management Control of Electronic Data Processing." A report prepared by the IBM Corporation. Technical Publications Department. White Plains, N.Y. 1965.

IBM Corporation. "The Considerations of Data Security in a Computer Environment."

"Invasion of Privacy." Hearings pursuant to S. Res. 39. 89th Congress, 1st Session, Feb. 18, 23–24, March 2–3, 1965. Part 2 (Ap. 13, 27–29, May 5–6, and June 7, 1965); Part 3 (July 13–15, 19–21, 27 and Aug. 9, 1965).

Isaacs, H. H. *User-Oriented Information Systems for State and Local Government.* A report prepared by System Development Corporation. 1965.

Miller, Roger F. "Confidentiality and Usability of Complex Data Bases." Social Systems Research Institute, University of Wisconsin. May 1967.

New York State. *Individual Liberties: The Administration of Criminal Justice.* A report prepared by the Temporary State Commission on the Constitutional Convention. Albany, N.Y. March 16, 1967.

New York State. *Security and Privacy.* A document prepared by the New York State Identification and Intelligence System.

Peters, Bernard. "Security Considerations in a Multi-Programmed Computer System." National Security Agency, Fort Meade, Md.

Petersen, H. E. and Turn, Rein. "System Implications of Information Privacy." RAND Corporation. April, 1967.

Rothman, Stanley. "Centralized Government Information Systems and Privacy." TRW Systems, September 22, 1966.

"Special Inquiry on Invasion of Privacy". (Hearings). 89th Congress, 1st Session, June 2, 3, 4, 7, 23 and September 23, 1965. Part 2, May 24, 1966.

U.S. Bureau of the Budget. *Report to the President on the Management of Automatic Data Processing in the Federal Government.* 98th Congress, 1st Session, March 4, 1965.

U.S. Bureau of Labor Statistics. *Implications of Automation and Other Technological Developments: A Selected Annotated Bibliography.* Washington, D.C.

Ware, W. H. "Security and Privacy in Computer System." RAND Corporation. April 1967.

Weissman, Clark. "Security Controls in the ADEPT-50 Time-Sharing System." System Development Corporation. May 1969.

IV. UNPUBLISHED MATERIALS

Baran, Paul. "Communications, Computers and People." California: Rand Corporation, 1965 (Mimeographed).

Babcock, J. D. "A Brief Description of Privacy Measures in the RUSH Time-Sharing System." Paper read at the 1967 Spring Joint Computer Conference, Atlantic City, N.J., April 18–20, 1967.

Bisco, Ralph L. "Urban Study Banks: A Preliminary Report." New York: Council of Social Science Data Archives, 1966 (Mimeographed).

Dennis, Jack B. and Glaser, Edward L. "The Structure of On-Line Information Processing Systems." (Mimeographed.)

Dunn, Edgar S. Jr. "The Idea of a National Data Center and the Issue of Personal Privacy." Presented before MENSA Society, N.Y. Oct. 21, 1966.

Fazar, Willard. "Federal Information Communities: The Systems Approach." A paper read at the 1966 Annual Meeting of the American Political Science Association, New York City, September 6–10, 1966. (Mimeographed.)

Gallagher, Cornelius. "Privacy and the National Data Center." Paper read at the Spring Joint Computer Conference, Atlantic City, N.J., April 18, 1967. (Mimeographed.)

Gallagher, Cornelius E. (Rep.-D. N.J.). Statement on Questions of Invasion of Privacy Relating to Establishment of National Data Center. Aug. 18, 1966.

Gill, William A. "Federal-State-Local Relationships in Data Processing." Paper read at the Conference on the Large-Scale Public EDP System, New York University, April 2, 1966.

Glaser, Edward L. "The Problems of Privacy in Remote-Access Computer System." October 3, 1966. (Mimeographed.)

Hazard, Geoffrey C. "The Sequence of Criminal Prosecution." Paper read before the National Symposium on Science and Criminal Justice, Washington, D.C., June 22–23, 1966. (Mimeographed.)

Lohman, Joseph D. "Changing Patterns of Crime." (Mimeographed.)

McDonell, R. E. "Cooperative Information Problems for Law Enforcement." White Plains, N.Y.: IBM Corporation. (Mimeographed.)

Mendelssohn, Rudolph C. "Proposed National Data Center—Items for Discussion at Symposium." New York: Council of Social Science Data Archives, 1967. (Mimeographed.)

Mindlin, Albert. "Confidentiality and Local Data Systems." Am. Stat. Ass'n Annual Meeting—12/27/67. Washington, D.C.

Mitchell, John F. "Communications Efficiency and Security." Presented at 74th Annual Conference IACP, Kansas City, September 1967.

Rothman, Stanley. "Privacy and Government Information Systems." Paper read at the Spring Joint Computer Conference, Atlantic City, N.J., April 18, 1967.

Shils, Edward. "Privacy and Power." A paper read at the 1966 Annual Meeting of the American Political Science Association, New York City, September 6–10. (Typewritten.)

Storer, Norman. "Large-Scale Data Collections and the Protection of Privacy." Social Science Research Council, 1967. (Mimeographed.)

Westin, Alan. "Legal Safeguards to Insure Privacy in a Computer Society." Paper read at the Spring Joint Computer Conference. Atlantic City, N.J., April 18, 1967. (Mimeographed.)

o

printed in CALIFORNIA OFFICE OF STATE PRINTING