Technical Report No. 13 (Revised)
July 1988

Standards for the Security and Privacy of Criminal History Record Information

— Third Edition —

SEARCH GROUP Inc.
The National Consortium for Justice Information and Statistics
925 Secret River Drive, Suite H • Sacramento, CA 95831 • (916) 392-2550

SEARCH GROUP, INC.

MEMBERSHIP GROUP

Chairman: Gary D. McAlvey **Vice Chairman: Maj. James Kinder**

Alabama: Maj. Jerry Shoemaker, Chief, Bureau of Investigation, Department of Public Safety
Alaska: John E. Angell, Dean, School of Justice, University of Alaska, Anchorage
Arizona: D.C. Britt, ACJIS Division Manager, Arizona Department of Public Safety
Arkansas: David Eberdt, Director, Arkansas Crime Information Center
California: Steve E. Kolodney, Director, Office of Information Technology, Department of Finance
Colorado: William Woodward, Director, Colorado Division of Criminal Justice, Department of Public Safety
Connecticut: Capt. George Moore, Connecticut State Police
Delaware: Cornelius A. Tilghman Jr., Executive Director, Delaware Justice Information System
District of Columbia: Shirley A. Wilson, Director, Office of Criminal Justice Plans and Analysis
Florida: Patrick J. Doyle, Director, Division of Criminal Justice Information Systems, Florida Department of Law Enforcement
Georgia: Thomas J. McGreevy, Division Director, Georgia Crime Information Center
Hawaii: Warren Price III, Attorney General
Idaho: Richard L. Cade, Deputy Director, Criminal Identification Bureau, Idaho Department of Law Enforcement
Illinois: Gary D. McAlvey, Chief, Bureau of Identification, Division of Forensic Services and Identification, Illinois Department of State Police
Indiana: Maj. James Kinder, Data Systems, Indiana State Police
Iowa: Carroll Bidler, Director, Administrative Services Division, Iowa Department of Public Safety
Kansas: Michael E. Boyer, Supervisor, Statistical Analysis Center
Kentucky: Gary Bush, Administrator, Records Section, Kentucky State Police
Louisiana: Dr. Hugh M. Collins, Chief Deputy Judicial Administrator, Supreme Court of Louisiana
Maryland: Paul E. Leuba, Director, Data Services, Department of Public Safety and Correctional Services
Massachusetts: Dr. Francis J. Carney Jr., Executive Director, Criminal History Systems Board
Michigan: Dallas G. Piper, Acting Division Commander, Central Records Division, Michigan Department of State Police
Minnesota: Kenneth A. Bentfield, Director, Office of Information Systems Management, Department of Public Safety
Mississippi: Sherry B. Morgan, Director, Justice Information Center, Department of Public Safety
Missouri: Dr. Robert J. Bradley, Director, Information Systems, Missouri Highway Patrol
Montana: Marvin Dye, Chief, Grant Administration Bureau, Montana Department of Justice
Nebraska: Gene Crump, Deputy Attorney General
Nevada: Wayne Teglia, Director, Department of Motor Vehicles
New Hampshire: Mark Thompson, Law Office Administrator, Attorney General's Office
New Jersey: Maj. Richard Jankowski, Supervisor, Records and Identification Section, New Jersey State Police
New Mexico: Irene Trujillo, Records Division Director, New Mexico State Police
New York: Owen Greenspan, Deputy Commissioner, Division of Criminal Justice Services
North Carolina: William C. Corley, Assistant Director, Division of Criminal Information, State Bureau of Investigation, Department of Justice
North Dakota: Robert Helten, System Specialist, Criminal Justice Training and Statistics Division, Office of the Attorney General
Ohio: Fred W. Engelman, Bureau Chief, Governor's Office of Criminal Justice Services, Department of Development
Oklahoma: Tom Heggy, Director, State Bureau of Narcotics
Oregon: Gerald C. Schmitz, Administrator, Information Systems Division, Oregon Executive Department
Pennsylvania: Dr. Alfred Blumstein, Dean, School of Urban and Public Affairs, Carnegie-Mellon University
South Carolina: James V. Martin, Director, Administrative Services, South Carolina Law Enforcement Division
South Dakota: Thomas J. Del Grosso, Administrative Services Agent, Division of Criminal Investigation, Criminal Justice Training Center
Tennessee: Arzo Carson, Director, Tennessee Bureau of Investigation
Texas: Rider Scott, General Counsel and Criminal Justice Advisor, Office of the Governor
Utah: Rolen Yoshinaga, Programmer/Analyst, Utah Commission on Criminal and Juvenile Justice
Vermont: Paul Stageberg, Director, Vermont Criminal Justice Center
Virginia: Richard N. Harris, Director, Department of Criminal Justice Services
Virgin Islands: George A. Farrelly, Safety and Security Officer, Virgin Islands Port Authority
Washington: George B. Tellevik, Chief, Washington State Patrol
West Virginia: Col. W.F. Donohoe, Superintendent, Department of Public Safety
Wisconsin: Stephen Puckett, Program Planning Analyst/Supervisor, Division of Corrections

At-large appointees
James R. Donovan, Director of Information Systems, U.S. Supreme Court
Dr. Charles M. Friel, Dean and Director, Criminal Justice Center, Sam Houston State University, Huntsville, Texas
Stephen Goldsmith, Marion County Prosecuting Attorney, Indianapolis, Indiana
Dr. Mark H. Moore, John F. Kennedy School of Government, Harvard University
Larry Polansky, Executive Officer, District of Columbia Court Systems
Judge Romae T. Powell, Fulton County Juvenile Court, Atlanta, Georgia
Presiding Judge Thomas J. Stovall Jr., 2nd Administrative Judicial District of Texas
Prof. George Trubow, Director, Center for Informatics Law, The John Marshall Law School

Staff
Gary R. Cooper, Executive Director
David J. Roberts, Deputy Director, Programs
George A. Buck, Deputy Director, Administration and Finance

117164

Technical Report No. 13 (Revised)

July 1988

Standards for the Security and Privacy of Criminal History Record Information

— Third Edition —

Report of work performed under Grant Nos. 82-BJ-CX-0010 and 87-BJ-CX-K079 from the Bureau of Justice Statistics, U.S. Department of Justice.

SEARCH Group, Inc.
The National Consortium for Justice Information and Statistics
925 Secret River Drive, Suite H • Sacramento, CA 95831 • (916) 392-2550

TABLE OF CONTENTS

SEARCH GROUP, INC.
LAW AND POLICY PROJECT ADVISORY COMMITTEE

♦ Chairman

Gary Bush
Administrator, Records Section
Kentucky State Police

♦ Members

D.C. Britt
ACJIS Division Manager
Arizona Department of Public Safety

Richard L. Cade
Deputy Director
Idaho Department of Law Enforcement

Dr. Hugh M. Collins
Chief Deputy Judicial Administrator
Supreme Court of Louisiana

Gene Crump
Deputy Attorney General
Nebraska Attorney General's Office

Patrick J. Doyle
Director, Division of Criminal Justice
Information Systems
Florida Department of Law Enforcement

David Eberdt
Director, Arkansas Crime Information Center

Fred W. Engelman
Bureau Chief
Governor's Office of Criminal Justice Services
Ohio Department of Development

Stephen Goldsmith
Prosecuting Attorney
Marion County, Indiana

Richard N. Harris
Director, Department of Criminal Justice Services
Virginia

Tom Heggy
Director, State Bureau of Narcotics
Oklahoma

Major Richard Jankowski
Supervisor, Records and Identification Section
New Jersey Division of State Police

Larry Polansky
Executive Officer
District of Columbia Court Systems

Judge Romae T. Powell
Fulton County Juvenile Court
Atlanta, Georgia

Rider Scott
General Counsel and Criminal Justice Advisor
Texas Office of the Governor

Prof. George Trubow
Professor of Law and Director
Center for Informatics Law
The John Marshall Law School

Irene Trujillo
Records Division Director
New Mexico State Police

Shirley A. Wilson
Director, Office of Criminal Justice
Plans and Analysis
Washington, D.C.

♦ Staff

Sheila J. Barton
Director, Law and Policy Program

Robert R. Belair
SEARCH General Counsel
Kirkpatrick & Lockhart

Thomas F. Wilson
Senior Writer

Paul L. Woodard
Senior Counsel

♦ Project Monitor

Carol G. Kaplan
Chief, Federal Statistics and Information
Policy Branch, Bureau of Justice Statistics
U.S. Department of Justice

PREFACE

Technical Report No. 13: Standards for the Security and Privacy of Criminal History Record Information is the culmination of a three-year effort by the SEARCH Membership Group to re-evaluate and revise national standards for handling criminal justice information. Originally formulated by SEARCH in 1975, the standards were updated in 1978. With the adoption, in July 1988, of the standards presented here, SEARCH has reaffirmed its long-standing commitment to the principle that the individual's right to privacy must be balanced with society's need for criminal history information.

As advocates of responsible criminal justice information law and policy, SEARCH has been committed to maintaining this balance since its formation in 1969. In 1970, SEARCH first published findings and recommendations regarding the security, privacy and confidentiality of information contained in computerized criminal history files (*Technical Report No. 2: Security and Privacy Considerations in Criminal History Information Systems).* Subsequent SEARCH documents provided guidance in establishing legislative and regulatory protections for criminal offender recordkeeping (*Technical Memorandum No. 3: A Model State Act for Criminal Offender Record Information* and *Technical Memorandum No. 4: Model Administrative Regulations for Criminal Offender Record Information*).

While serving the needs of criminal justice practitioners, these publications were limited to addressing prototype criminal history exchange systems and rap sheet information. The scope of the 1975 publication of *Technical Report No. 13* surpassed the previous documents in that it was the first comprehensive statement of SEARCH's recommendations for safeguarding the security and privacy of all criminal justice information.

Technical Report No. 13 addresses important criminal justice issues and as changes in society affect these issues, SEARCH has responded by revising *Technical Report No. 13.* For example, the phenomenal growth of technology has enabled criminal justice agencies to collect, store, analyze and disseminate a vast volume of records and statistics, but this growth has lead to justifiable concerns that the security and integrity of the information — as well as the rights of the person to whom the information relates — be protected. Dissemination of inaccurate data, the use of data for wrongful purposes, and inappropriate harm to the subject of a criminal history record are all consequences of a failure to protect data.

This third edition of *Technical Report 13* sets forth 19 standards which are intended to guide those responsible for developing legislation and regulations regarding the security, privacy and confidentiality of criminal history information. New standards have been added to address the growing concern with noncriminal justice access to criminal history records and the establishment of the Interstate Identification Index (III). The extensive commentary that accompanies each standard will aid the reader in understanding underlying policies and implications.

This revised edition was introduced by the SEARCH Law and Policy Project Advisory Committee (see page iii), and was unanimously approved by the SEARCH Membership Group at its Annual Meeting in July 1988. The report represents a deliberative, objective process which has resulted in definitive, cogent standards for managing criminal history information. Three years of discussions and analysis have resulted in the revised *Technical Report No. 13;* the SEARCH Membership Group received input from both inside and outside of the criminal justice community. Work on revising the standards was completed under a grant from the Bureau of Justice Statistics, U.S. Department of Justice.

The goal of SEARCH in presenting this report is to provide a comprehensive approach to criminal history information policy that is based upon articulated standards. This edition of *Technical Report No. 13* sets forth these standards in a pragmatic and concise manner, thus allowing policymakers to effectively apply the standards to fit the needs of their jurisdictions. The efforts of the Law and Policy Committee in realizing this goal are to be commended.

INTRODUCTION

In October 1975, SEARCH Group, Inc. (SEARCH) published a technical report containing comprehensive standards for the handling of criminal justice information titled *Technical Report No. 13: Standards for Security and Privacy of Criminal Justice Information* (*Technical Report No. 13* or *Report*). As originally published, the *Report* contained 25 standards for inclusion in federal and state legislation which, in conjunction with recommended agency regulations and operational procedures, sought to establish a national, interstate criminal justice information system and ensure the security, accuracy, completeness and confidentiality of criminal justice information. In addition, SEARCH intended that *Technical Report No. 13* should serve as a guide for officials to use in preparing state legislation and state, local and individual agency regulations and guidelines. Two years later, in 1977, SEARCH issued a second edition of *Technical Report No. 13*. The revised edition included an expanded commentary, but left the 25 original standards intact.

When adopted in 1975, the 25 original standards represented a distillation of six years of research by SEARCH and its predecessor, Project SEARCH, with respect to law and policy as it then related to criminal justice information. The thrust of the standards in *Technical Report No. 13* was threefold:

1. to establish a national, interstate criminal justice information system;
2. to ensure the security, accuracy and completeness of the information in that system; and
3. to ensure fairness, confidentiality and privacy with respect to record subjects.

Background of Technical Report No. 13

Project SEARCH was created in 1969 under a grant from the Law Enforcement Assistance Administration (LEAA). In many respects, the grant was a response to a concern that criminal justice agencies in many states were spending relatively large amounts of money on relatively experimental and untested automated information systems. In its early years, Project SEARCH helped to promote a more orderly and efficient means of developing, evaluating and implementing automated information systems. Project SEARCH's first major effort was the development and successful demonstration of a prototype computer-based information system in seven states for the interstate exchange of criminal history records. That prototype system eventually encompassed 20 states and, in a very real sense, was the forerunner of today's Interstate Identification Index (III).

In developing that demonstration system, it became clear to the members of Project SEARCH that security, privacy and confidentiality issues regarding criminal justice information would require special attention. In 1969, Project SEARCH established a permanent committee on security and privacy to study these problems and to develop recommendations. In July 1970, Project SEARCH published the committee's findings and recommendations as *Technical Report No. 2: Security and Privacy Considerations in Criminal History Information Systems (Technical Report No. 2)*. Shortly thereafter, Project SEARCH published *Technical Memorandum No. 3: A Model State Act for Criminal Offender Record Information (Technical Memorandum No. 3)* and *Technical Memorandum No. 4: Model Administrative Regulations for Criminal Offender Record Information (Technical Memorandum No. 4)*. By 1975, however, it had become clear, as the commentary to *Technical Report No. 13* noted, that "none of these documents [*Technical Report No. 2* and *Technical Memoranda 3* and *4*] fully set out" Project SEARCH's then-current thinking with respect to criminal justice information policy. "For this reason, SGI developed and published *Technical Report No. 13...* ."

Impact of Technical Report No. 13

By any measure, the standards in *Technical Report No. 13* have had an important impact upon law and policy with respect to criminal justice information. The standards served in large measure as a basis for the LEAA's development of comprehensive regulations for criminal history record information adopted in March 1976 ("Justice Department Regulations").[1] The official appendix to those regulations, as published in the *Code of Federal Regulations*, expressly states:

[1] 28 C.F.R. Part 20.

> In preparing the plans required by these regulations, States should look for guidance to Project SEARCH: *Security and Privacy Considerations in Criminal History Record* [sic] *Systems, Technical Reports No. 2* and *No. 13*; ...[2]

Together, *Technical Report No. 13* and the Justice Department Regulations have had a significant effect on state criminal history record law. For example, in 1974, one year prior to publication of *Technical Report No. 13*, statutes in only 24 states regulated the dissemination of criminal history record information. By 1984, 52 states and territories regulated such dissemination. In 1974, statutes in only 12 states gave a record subject the right to inspect his criminal history record information. By 1984, 53 jurisdictions had adopted such provisions. In 1974, statutes in only 14 states set standards for accuracy and completeness. By 1984, 51 jurisdictions had adopted such standards. In 1974, statutes in only 12 states prescribed security safeguards for criminal justice information systems. By 1984, 38 jurisdictions had adopted such provisions. In 1974, statutes in only six states provided civil remedies for violations of record-keeping standards. By 1984, 36 states had adopted such provisions. And finally, in 1974, statutes in only 18 states imposed criminal penalties for criminal justice record violations. By 1984, 43 jurisdictions had adopted such provisions.

Technical Report No. 13 has also had a significant impact on the form that the emerging national criminal history exchange system is taking. *Technical Report No. 13* called for the establishment of a national, interstate system for the exchange of criminal justice record information centered around a national index which would "point" authorized requesters to records held in particular states. Today, that index is becoming a reality in the form of the III.

Recent Developments Call for New Standards

It is hardly surprising that, in the 13 years from 1975 to 1988, many new technological, political and legal developments have occurred which make it appropriate, indeed, necessary, for SEARCH to adopt comprehensive, new standards. There have been, for example, significant improvements in the accuracy, completeness and timeliness of criminal history record information and, concomitantly, advances in the development of techniques which have proven to be effective in improving data quality.[3] Although the extent and nature of progress since 1975 is not free from controversy, most researchers have little doubt that, especially in some states, very significant progress has been made. The emergence of techniques which have proven to be effective in improving data quality make it more appropriate than it was in 1975 for SEARCH to adopt standards which identify, with specificity, techniques which should be used to improve data quality. Improvements in data quality also provide a basis to relax confidentiality safeguards because today there is more reason to believe that when records are released, they will be accurate and complete.

Another development that has encouraged SEARCH to consider the adoption of new standards is the mushrooming demand by noncriminal justice agencies for access to, and use of, criminal justice information. SEARCH's 1985 survey of state repositories concluded that, "In a majority of states, however, the processing of noncriminal justice inquiries represents a significant portion of total processing workloads."[4] Some part of this increased demand is a result of an increase in litigation against employers under the "negligent hiring" doctrine. The negligent hiring doctrine, in some circumstances, makes employers liable for the criminal acts of their employees if the employer fails to make inquiries about the employee's or applicant's prior criminal history record.[5]

National security concerns also seem to be fueling continued, significant increases in the already massive volume of federal noncriminal justice requests for access to criminal history records for employment and security clearance screening purposes. For these and other reasons, the volume of requests for records from noncriminal justice users continues to mount. For example, the United States Congress' Office of Technology Assessment (OTA) found that, in 1981, about 53 percent of all requests for criminal history record information to the FBI's Identification Division were made by

---

[2] 28 C.F.R. Part 20 Appendix § 20.22(a).

[3] U.S., Department of Justice, Bureau of Justice Statistics, *Data Quality of Criminal History Records*, Criminal Justice Information Policy Series, NCJ-98079 (Washington, DC: U.S. Government Printing Office, October 1985), pp. 17-29.

[4] SEARCH Group, Inc., "State Criminal History Record Repositories," Draft Report (1986), p. 19.

[5] U.S., Department of Justice, Bureau of Justice Statistics, *Privacy and the Private Employer*, Criminal Justice Information Policy Series, NCJ-79651 (Washington, DC: U.S. Government Printing Office, November 1981), pp. 42-46.

noncriminal justice agencies — primarily federal "national security" agencies, such as the Department of Defense.[6] Most experts expect that demands for access from various noncriminal justice users will continue to grow.

Another important development in the last 13 years that encourages SEARCH to adopt new standards has been the increased use, in fact the now near-universal use, of automated information technology. By 1985, for example, all but five states had automated at least part of their criminal history record system and three of those states indicated that automation would begin in 1987. Use of automated information systems often improves data quality. This technology, however, also makes it easier and cheaper to collect, store and disseminate data.

Another development that is relevant to SEARCH's consideration of new standards has been the emergence of automated, name-indexed criminal record systems in settings where manual and non-name-indexed systems had previously been the norm. Court docket systems and police blotter systems are perhaps the two best examples. The emergence of automated, name-indexed newspaper morgues and other private sector databases is a related development.

Still another new technology that provides a basis for changes in policy is the emergence of Automated Fingerprint Identification Systems (AFIS). These systems permit the automated, positive identification of individuals on the basis of fingerprints, including latent (crime scene) prints. AFIS promises to vastly improve the reliability and utility of criminal history record checks. The emergence of even newer identification systems based on DNA typing data and other biometric identifiers also promise improvements in reliability and efficiency.

Another factor which encourages the adoption of new standards are research findings indicating that rehabilitation programs often do not work and that, instead, criminal recidivism rates for many types of offenders tend to stay high from the offender's late juvenile years through the offender's mid-to-late-20s.[7] Moreover, these new research findings indicate that a relatively small percentage of chronic, violent offenders account for a disproportionately large percentage of crime. For example, studies suggest that just over 20 percent of offenders commit over 60 percent of all homicides, over 75 percent of all rapes, nearly 75 percent of all robberies, and 65 percent of all aggravated assaults.[8] Based on research findings such as these, a credible empirical argument can be made that confidentiality safeguards should be relaxed for records relating to recent arrests and, particularly, convictions.

Still another factor that is influencing the adoption of new standards has been a steady erosion of the constitutional basis for the confidentiality of criminal history record information. In 1975, when *Technical Report No. 13* was published, the United States Court of Appeals for the District of Columbia Circuit had just issued two major decisions suggesting that constitutional interests are implicated when criminal history record information is disseminated.[9] One year after publication of *Technical Report No. 13*, however, the United States Supreme Court published *Paul v. Davis*.[10] In *Paul*, the Supreme Court rejected a record subject's claim that a sheriff's department's public dissemination of his name and photo as an "active shoplifter" is the kind of dissemination which violates an individual's constitutional right of privacy. The plaintiff had been arrested for shoplifting some 18 months earlier but had never been convicted, and the charges were still pending. The court rejected Davis' claim, stating that:

> [Davis] claims constitutional protection against the disclosure of the fact of his arrest on a shoplifting charge. His claim is based not upon any challenge to the State's ability to restrict his freedom of action in a sphere contended to be "private," but instead on a claim that the State may not publicize a

---

[6] U.S., Congress, Office of Technology Assessment, *An Assessment of Alternatives for a National Computerized Criminal History System*, OTA-CIT-161 (Washington, DC: U.S. Government Printing Office, October 1982), p. 176.

[7] R. Martinson, "What Works?: Questions and Answers About Prison Reform," *The Public Interest* 35 (Spring 1974) : 22; U.S., Department of Justice, Bureau of Justice Statistics, *Examining Recidivism*, Special Report, NCJ-96501 (Washington, DC: U.S. Government Printing Office, February 1985), p. 1.

[8] U.S., Department of Justice, Bureau of Justice Statistics, *Report to the Nation on Crime and Justice: The Data*, Bulletin, NCJ-87068 (Washington, DC: U.S. Government Printing Office, October 1983), p. 34.

[9] *Menard v. Saxbe*, 498 F. 2d 1017, 1026 (D.C. Circ. 1974), and *Tarlton v. Saxbe*, 507 F. 2d 1116, 1122-23 (D.C. Circ. 1974).

[10] 424 U.S. 693 (1976).

> record of an official act such as an arrest. None of our substantive privacy decisions hold this or anything like this, and we decline to enlarge them in this manner.[11]

Today, *Davis* continues to be good law. Indeed, in October 1987, the District of Columbia Circuit Court of Appeals issued its long-awaited decision on whether the FBI has authority under the federal Freedom of Information Act to withhold criminal history record information from the press and the public.[12] The Court of Appeals, in an opinion that is sure to have far-reaching implications, effectively held that federal agencies must disclose criminal history record information inasmuch as the component parts of the record, such as police docket entries or court docket entries, are already in the public domain. In light of these developments, there are few, if any, court-imposed bars to the disclosure of otherwise accurate or complete criminal history record information. This is a dramatically different legal environment than existed in 1975 and contributes to SEARCH's determination to reconsider its criminal justice information standards.

A final factor that encourages SEARCH to adopt new standards is the continued erosion of statutory confidentiality protections for criminal history record information. Since 1979, several states, including, most notably, Florida and Oklahoma, have adopted open record statutes under which the public can obtain virtually all criminal history record information.[13] In addition, in recent years, legislatures in many states have adopted legislation which authorizes or requires state repositories and/or other criminal justice agencies to make criminal history record information available to particular types of noncriminal justice requesters for particular purposes. Most common are statutes permitting or requiring the release of criminal history information for background investigations for individuals who work with children or who work in other kinds of sensitive positions.[14]

The Congress has also made piecemeal exceptions to comprehensive confidentiality safeguards with respect to criminal history information. Today, federally-held criminal history information can be released for background investigations for employment at certain kinds of banking institutions and securities organizations.[15] In 1985, moreover, the Congress enacted the Security Clearance Information Act (SCIA), which requires state and local criminal justice agencies to release criminal history record information to certain federal agencies for national security background checks.[16] In 1986, Congress enacted the Immigration Reform Act, which promises to unleash a torrent of requests to federal, state and local criminal justice agencies for criminal justice information about illegal aliens who are applying for eligibility for citizenship under the Immigration Reform Act program.[17]

Principles of Revised Standards

The revised standards reflect several goals that were either not reflected in the original standards or were of less importance in those standards, as follows:

- that the states should have exclusive control over criminal history information that they create or receive, except for such limitations as may be necessary in order to participate effectively in an interstate program for the exchange of criminal history information or for national security purposes;
- that noncriminal justice agencies may have a legitimate need for access to criminal history information;
- that insofar as is possible, all criminal history information should be disseminated only on the basis of positive identification by means of fingerprints;
- that state and local agencies should implement safeguards in order to enhance the security of manual and automated criminal justice information systems;
- that agencies should implement certain enumerated programs that have proven to be effective in improving the accuracy, completeness and timeliness of criminal justice information;

---

11 Id., p. 713.

12 *The Reporters Committee for Freedom of the Press v. U.S. Department of Justice*, 831 F. 2d 1124 (D.C. Circ. 1987), *rehearing denied* 831 F. 2d 1124 (1987).

13 U.S., Department of Justice, Bureau of Justice Statistics, *Public Access to Criminal History Record Information*, Criminal Justice Information Policy Series, NCJ-111458 (Washington, DC: U.S. Government Printing Office, November 1988), pp. 19-20.

14 Ibid., p. 29.

15 15 U.S.C. § 78q(f)(2).

16 Pub. L. No. 99-169, 99 Stat. 1009, codified in part at 5 U.S.C. § 9101.

17 Pub. L. No. 99-603, 100 Stat. 3359.

- that agencies should implement a regular program of training with respect to the handling of criminal history information;
- that agencies may, at their discretion, charge fees to requesters, other than criminal justice agencies, for access to criminal history information, except that fees should not be charged for processing III inquiries for noncriminal justice purposes;
- that agencies should establish programs for auditing criminal history information systems; and
- that the states should participate fully in the Interstate Identification Index, as set forth in Standard 15 herein.

TEXT OF STANDARDS AND OFFICIAL COMMENTARY

Standard 1. State Authority

1.1. The authority of state legislatures to enact legislation governing the maintenance, use or dissemination of criminal justice information within a given state is based upon the plenary powers of the states, including the police powers of the states, reserved by the Tenth Amendment to the states.

Commentary

This Standard recognizes the authority of state legislatures to enact legislation governing the activities of state and local criminal justice information systems.

Standard 1.1 describes the powers of state legislatures to enact legislation governing the activities of criminal justice information systems within the individual states. The Tenth Amendment to the Constitution states that all powers not delegated by the Constitution to the federal government nor prohibited to the states are reserved to the states. Thus, except to the extent that the Congress may regulate state agencies and activities pursuant to express or necessarily implied constitutional grants of power (for example, such as the Congress did in 1985 in adopting the federal Security Clearance Information Act (SCIA),[18] which requires state and local agencies to make criminal history record information available to certain federal agencies for national security purposes in certain circumstances), each state possesses plenary power to regulate its own criminal justice agencies and activities.

1.2. States should exercise primary authority over the maintenance, use and dissemination of criminal justice information which agencies located within the state create or receive, subject only to such limitations as may be necessary in order to participate effectively in an interstate program for the exchange of criminal justice information or for national security purposes.

[18] Pub. L. No. 99-169, 99 Stat. 1009.

Commentary

States not only have the constitutional authority to govern the maintenance, use and dissemination of criminal justice information, but as a policy matter, states should exercise that authority. Accordingly, these standards — with the exception of Standard 15 covering the Interstate Identification Index — convey recommendations to state legislatures. The standards can be adopted *in toto*, in which case the resulting legislation would establish a comprehensive arrangement for the handling of criminal justice information and, in particular, criminal history record information. On the other hand, the standards are drafted in such a way that state legislatures can selectively adopt particular standards or parts thereof depending upon circumstances in their individual states.

States and localities operate the vast majority of law enforcement agencies, courts and correctional facilities. It has been estimated that about 95 percent of the criminal justice activities in the nation are state and local in character. Thus, state and local criminal justice agencies collect, maintain, use and disseminate the vast bulk of criminal justice information. Accordingly, states and their localities should take the primary role in the design and regulation of criminal justice information policies. Second, the emergence of central state repositories makes it more appropriate than ever that states take the primary role in the management of criminal justice information.

Standard 1.2 provides that a state should exercise authority not only over criminal justice information which agencies within the state create (at least so long as the information is maintained in the state), but also over criminal justice information created by agencies outside the state when the information is transferred into the state. In other words, under this standard, the "recipient" state, not the "donor" state, should set policies for maintenance, use and dissemination.

Two considerations justify this approach. First, this approach recognizes that an agency in the recipient state has obtained the record in order to make a determination about a record subject located in the state. Standard 1.2 reflects the view that decisions about whether past criminal conduct should influence hiring, licensing or other determinations should be made by the legislatures and other policymakers in the state where the determination

is to be made. Second, as a practical matter, agencies receiving a record from out-of-state cannot reasonably be expected to know the law of the donor state; or, even if they are familiar with out-of-state law, they cannot be expected to establish a system whereby out-of-state information is permanently "tagged" with an out-of-state label.

Standard 1.2 recognizes two exceptions to the principle that the state maintaining the data should set the rules for the maintenance, use and dissemination of the data. First, the standard recognizes that compliance with national standards may be necessary in order to permit a state to participate effectively in an interstate program for the exchange of records. This approach parallels the approach taken in Standard 15 governing the III and reflects the view that, if a national exchange system is to be successful, national rules must provide compatibility and assure users that the system will provide access to at least a reasonable amount of data.

Second, Standard 1.2 recognizes that state rules for maintenance, use and dissemination may, where necessary, be pre-empted when information is sought for genuine national security purposes. This approach is reflected in the federal SCIA, which requires state and local agencies to disclose criminal history record data to certain federal agencies for certain national security purposes. Even in this situation, however, state and local agencies retain substantial discretion and the SCIA pre-empts state law only to the extent necessary to safeguard national security interests.

Standard 2. Definitions

2.1. For purposes of these Standards, "criminal justice information" includes the following kinds of information:

(a) "correctional and release information," defined as information or reports on individuals compiled in connection with bail, pretrial or post-trial release proceedings, pre-sentence investigations, proceedings to determine physical or mental condition, participation by inmates in correctional or rehabilitative programs, or probation or parole proceedings;

(b) "criminal history record information," defined as information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations or other formal criminal charges, and any disposition arising therefrom, including sentencing, correctional supervision and release;

(c) "criminal index information," defined as information about an individual about whom criminal history record information is maintained by one or more state central repositories and/or the Federal Bureau of Investigation (FBI), including an identification of the jurisdiction and agency maintaining the criminal history record information;

(d) "criminal intelligence information," defined as information on identifiable individuals compiled in an effort to anticipate, prevent or monitor possible criminal activity;

(e) "criminal investigative information," defined as information on identifiable individuals compiled in the course of the investigation of specific criminal acts;

(f) "disposition," defined as information disclosing that a decision has been made not to bring criminal charges or that criminal proceedings have been concluded, abandoned or indefinitely postponed; or information relating to sentencing, correctional supervision, release from correctional supervision, the outcome of appellate review of criminal proceedings or executive clemency;

(g) "identification record information," defined as fingerprint classifications and other physical descriptive data concerning an individual to the extent that it does not include any indication or suggestion that the individual has at any time been suspected of or charged with a criminal offense;

(h) "nonconviction information," defined as information without disposition if an interval of one year has elapsed from the date of arrest and no active prosecution of the charge is pending; or information disclosing that a criminal justice agency has elected not to refer a matter to a prosecutor, or that a prosecutor has elected not to commence criminal

proceedings, or that proceedings have been indefinitely postponed, as well as all acquittals and all dismissals; and

(i) "wanted person information," defined as identification record information on an individual against whom there is an outstanding arrest warrant, including the charge for which the warrant was issued, and information relevant to the individual's danger to the community and any other information that would facilitate the apprehension of the individual.

Commentary

Standard 2.1 defines the types of information that are included in the term "criminal justice information" and thus are covered by the standards. Paragraphs (b), (f) and (g), which define "criminal history record information," "disposition" information and "identification record information," along with paragraph (h), which defines "nonconviction information," collectively include all of the elements of a traditional criminal history record or "rap sheet." All four of these terms are defined in a manner that is substantively similar to the definitions of these terms in the Justice Department Regulations, 28 C.F.R. § 20.3(b), (e) and (k). It should be noted that identification record information, as defined in paragraph (g), includes not only fingerprint classifications, but also retina pattern data, voice print data, DNA typing data and other kinds of physical descriptors.

Correctional and release information, as defined in paragraph (a), includes information about formal criminal justice events, such as bail reports, presentence reports and parole reports; and "informal" events or activities, such as information about participation in correctional or psychological treatment programs or prison employment. Some of the formal reports may be part of the subject's conviction record. To the extent, however, that correctional and release information is not a part of a conviction record, this information is subject, under the Standards, to strict dissemination standards.

The term "criminal index information" in paragraph (c) refers to identification information used to "point" an authorized requester to a jurisdiction maintaining criminal history record information about a record subject. In this sense, although criminal index information consists largely of identification information, its maintenance in a criminal index information system indicates that there is a criminal history record. For this reason, and in view of the fact that the term "criminal index information" is used in Standard 15's discussion of the Interstate Identification Index, it is appropriate that the term be defined.

Two other types of information subject to the Standards are "criminal intelligence information" (paragraph (d)) and "criminal investigative information" (paragraph (e)). Both definitions relate to prearrest investigative information. They are distinguished, however, in that "intelligence" information relates to possible or suspected unspecified criminal acts. By contrast, "investigative" information relates to a suspected, specific criminal act.[19] Both of these definitions relate to records or information compiled on identifiable individuals. The term "individual" is used to refer to natural persons and does not include corporations or other legal persons.

It should be noted that the term "disposition" defined in paragraph (f) relates to more than simply the outcome of the initial prosecution stage of criminal proceedings. The term also includes information relating to sentencing, correctional supervision, executive clemency and appellate review of criminal proceedings, all of which relate to post-prosecution proceedings. Thus, "disposition" should be understood to mean the formal conclusion of each stage of a criminal case. It follows, then, that many cases will have more than one disposition.

The definition of "wanted person information" in paragraph (i) is restricted to instances where an arrest warrant has been issued and the information includes a statement of the charges for which the warrant was issued. Of course, restrictions based on state law may be applicable to this type of information. Although the wide public dissemination of wanted person information may harm a record subject, two factors make it appropriate to treat this information differently from criminal history record information or intelligence and investigative information. First, the public's interest in apprehending the subject and the need to alert the public to a potential danger create an especially compelling state interest in the disclosure of this information. Second, the subject can be said to have "waived" some degree of his privacy interest by failing to answer the warrant.

---

[19] See U.S., Department of Justice, Bureau of Justice Statistics, *Intelligence and Investigative Records*, Criminal Justice Information Policy Series, NCJ-95787 (Washington, DC: U.S. Government Printing Office, February 1985), p. 9.

2.2. For purposes of these Standards, "criminal justice agency" is defined as:

(a) courts;

(b) a government agency or any subunit thereof which performs the administration of criminal justice pursuant to a statute, local ordinance or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice; and

(c) any other agency or organization, including a private organization not covered by paragraphs (a) or (b), which, by contract with a covered agency, performs an activity covered in section 2.3, but only to the extent of that activity.

2.3. The "administration of criminal justice" is defined as the performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision or rehabilitation of accused persons or criminal offenders. The administration of criminal justice includes criminal identification activities and the collection, storage and dissemination of criminal history record information. State and federal inspectors general offices are included.

Commentary

Standard 2.2 defines "criminal justice agency" and "administration of criminal justice" to include any adult court with criminal or civil jurisdiction and any other governmental agency, or subunit thereof, that is principally engaged in specified activities related to the administration of criminal justice, as well as entities under contract to the agency which perform such activities on behalf of the agency. Thus, all adult courts qualify as criminal justice agencies. Other agencies must meet a three-part test to qualify. First, the agency must be characterized as "governmental;" that is, the head of the agency must be an elected or appointed official or responsible to such an official. Second, pursuant to statute or executive orders, the agency must perform one or more of the criminal justice activities set forth in the definition. If the agency's criminal justice activities are authorized by the state's constitution, the authorization is also effective. Third, these activities must be the agency's principal function; that is, they must occupy more than one half of the agency's time or resources. Even if an entire agency does not qualify as a criminal justice agency, it is possible that a subunit may qualify.

Several other points should be emphasized. First, the criminal justice-related activities set out in the definition do not include crime prevention activities. Accordingly, activities, such as drug addiction programs aimed at crime prevention through reduction of drug-related crimes, would not qualify the agencies operating the programs for access to criminal history records. Second, criminal justice-related activities do not include criminal defense. Thus, private defense attorneys and members of public defender offices would not be considered criminal justice officials. Criminal history records, however, must generally be made available to them under court order, pursuant to state statute or through the record subject.

Third, the criminal justice activities set out in the definition include criminal identification functions and the collection, storage and dissemination of criminal justice information. This means that data processing activities supportive of criminal justice agencies qualify an agency as a criminal justice agency if those activities constitute the principal function of the data processing unit. Thus, a state central data processing unit or a distinct subunit thereof, performing identification and record storage and dissemination services for criminal justice agencies, may be considered a criminal justice agency if those services constitute the principal part of its total activities.

Finally, throughout the Standards, the term "criminal justice purpose" is used. Whenever used, this term should be understood to include and be limited to the activities set forth in Standard 2.3. In other words, a criminal justice purpose is any activity whose goal is the detection, apprehension, detention, pretrial release, prosecution, adjudication, correctional supervision or rehabilitation of accused persons or criminal offenders.

2.4. "Central state repository" is defined as an agency, department, board, commission, office or other unit of state government with authority to maintain a central data facility of criminal justice information which will include criminal history record information and may include identification record information or other types of criminal justice information for the purpose of collecting, maintaining and disseminating, as appropriate, on behalf of the state, criminal justice information to qualified recipients, as prescribed by state law or other appropriate law.

Commentary

In 1987, Nevada became the last state to establish a central criminal history record repository. These repositories are charged with the responsibility of maintaining files of criminal arrest and charge data contributed by local law enforcement agencies and case disposition data submitted by prosecutors, courts and correctional agencies, and providing offender criminal history records, commonly called "rap sheets," to criminal justice agencies throughout the state that require such records for use in the discharge of their duties. Although most of the repositories maintain other types of records and provide other types of criminal justice services, it is the importance of the basic criminal history record that has secured for the repositories the prominence in the criminal justice system that they now enjoy. Criminal history records are generally thought to be the most widely used records within the criminal justice process. Throughout the system, these records are relied upon as a primary source of information vital to decisionmaking and the exercising of discretion concerning the processing of criminal defendants.

About one-half of the repositories owe their founding to the upgrading of previously existing state bureaus of identification. Many of these bureaus were initially established as long as 50 or 60 years ago to serve as the state repository of criminal fingerprints and to provide criminal identification services and investigative assistance to law enforcement agencies within the state. By the 1960s, in some of the states, particularly the larger, more populous states, these bureaus had become important sources of criminal arrest record data for prosecutors and courts, as well as law enforcement agencies, and had begun collecting disposition data and assembling and providing criminal history records. A few of the largest bureaus had begun to use computers to automate their databases and the processing of inquiries. It was the establishment of the LEAA in 1968, however, and the infusion of substantial federal assistance by LEAA aimed at the improvement of the state identification bureaus, that marked the beginning of the development of today's criminal record repositories. Although LEAA did not require each state to establish a central criminal record repository, it did strongly encourage the establishment of such agencies.

As a result, the 1970s were a period of great progress in the evolution of the present day repositories, with the establishment of new repositories in many states and the implementation of programs to improve existing repositories in other states. A 1986 SEARCH survey of repositories indicates that at least 16 of the repositories were established after 1970.[20] In many other states, existing bureaus of identification were designated as central record repositories and were given the necessary additional responsibility and authority. During this period, the state legislatures were active in developing and enacting new criminal history record laws that emphasized the importance and authority of the repositories and imposed reporting requirements on local criminal justice agencies.[21]

2.5.

(a) "Seal" is defined to mean prohibiting access to criminal history record information except to: criminal justice agencies for record management purposes; government officials and criminal justice officials for criminal justice employment determinations; the record subject; a party for an authorized research or statistical purpose; and a party authorized access to a record by statute or a court order.

(b) "Purge" is defined to mean destroying, blotting out, striking out or effacing so that no trace as to the individual's identification remains. Destruction of personal identifiers so that the record or entry can never be associated with an individual is a form of purging.

Commentary

Standard 2.5(a) defines the term "seal" to denote two characteristics: (1) the sealed record or entry continues to exist; and (2) virtually all dissemination of the sealed record or entry is prohibited. This approach distinguishes a sealed record from a purged (destroyed) record, and from a record that is merely subject to certain confidentiality safeguards and dissemination limitations.

The definition of seal is consistent with the practice in many central state repositories. The heart of a sealing

---

20 See note 4, table 1, p. 4.

21 U.S., Department of Justice, Bureau of Justice Statistics, *Compendium of State Privacy and Security Legislation, 1984 Edition: Overview*, NCJ-98077 (Washington, DC: U.S. Government Printing Office, September 1985).

action, in most states, is to remove the record or a specific entry on the record from routine access within the repository and routine dissemination outside the repository. The information, once sealed, is available only in exceptional circumstances. [Note that under Standards 15.1 and 15.4, index information in the III would not reflect a record if the record has been sealed.] Various levels of security may be applied when the sealed data are under the custody of specific repository personnel or, in an automated environment, when the data are accessible only by selected terminals. In any event, the effect of the seal from the point of view of the recordkeeper is to ensure that reasonable safeguards against improper disclosure or dissemination are in place.

The definition of seal contemplates that disclosure will occur in only five circumstances. First, criminal justice agency employees (as well as contractors or agents who are performing microfilming or other record management functions) are permitted access, provided that they have a demonstrated need for access to the data in order to accomplish a proper record management function, such as updating or correcting an entry. This provision represents a common-sense, practical accommodation to the reality that some employees or agents of the agency maintaining a record must, of necessity, see the record. Those persons, however, are permitted access only in connection with recordkeeping operations.

Second, government criminal justice officials are permitted access to sealed data for criminal justice employment screening determinations. This provision would give criminal justice officials access to sealed data, as well as give the President, governors, other executive officials and legislative officials access to sealed data in connection with appointment decisions for judges, police commissioners and other executive-level criminal justice officials. The reason that access to sealed data is appropriate is that this data often will be relevant to criminal justice employment decisions. It is important to assure that individuals charged with upholding the law do not themselves have a history of violations of law; moreover, public confidence in the integrity and rectitude of criminal justice officials may be adversely affected if these officials have prior records.

Third, the definition contemplates that the record subject will have access to his sealed data. Such access includes a right to obtain a copy of the record. The definition assumes that the purposes served by sealing a criminal history record are not served by cutting off a record subject's access rights. This approach is consistent with most existing state statutory sealing provisions. In most states, a subject, upon proper identification, is entitled to review the contents of his sealed information — presumably for purposes of ascertaining the record's completeness and accuracy.

Fourth, the definition contemplates that persons who will use the sealed data for authorized research and statistical purposes are also permitted access. The term "authorized research and statistical purposes" contemplates that the applicant will comply with Standard 13.2 regarding researcher access and with the standards for researcher access and use of identifiable criminal justice data adopted by the Justice Department at 28 C.F.R. Part 22.

Fifth, the definition assumes that any party with a court order is permitted access. Naturally implicit in this authorization is the right of a court to conduct an *in camera* review of the record prior to issuing the order. This provision provides a "safety valve" for access in various situations where there is a compelling need for access.

Methods used by recordkeepers to accomplish a sealing vary. The two most common approaches, however, are both consistent with Standard 2.5(a). Strict physical segregation of a record is the first approach. Agencies remove all information pertaining to the sealed record from agency records and secure the sealed data in a separate file. The file usually contains other sealed records and is maintained under lock and key. Often agencies assign responsibility for record maintenance and security to certain designated personnel.

Agencies also use a second, less restrictive approach. Agencies maintain the sealed data alongside nonsealed data. Agencies, however, use physical or automated shielding or logical separation techniques to prevent the data from being seen during routine passes through the file. In automated systems, the task of separating the data is made easier. The sealed data remains in the system but can be retrieved only by personnel who are authorized to use particular terminals and/or retrieval directions.

Standard 2.5(b) defines the term "purge" in a literal and common-sense manner — to destroy. To accomplish a purge, agencies may often destroy an entire record, including fingerprints, photographs and arrest and disposition data; or agencies may retain a record, but entries within the record are purged. This is a common occurrence when multiple charges are part of the same case, not all of which resulted in a disposition favorable to the subject. A criminal case that resulted in two charges being filed, one of which ended in conviction and one of which ended in a nonconviction, for example, might be handled in the following manner: identification data including the fingerprint card is retained; however, the nonconviction data and any other data which

refer to the nonconviction are erased or otherwise destroyed. The term "expunge" is not used in these definitions because the term has different and sometimes opposing meanings in various states.

Standard 3. Information Excluded from Coverage

3.1. The Standards should not apply to:

(a) chronologically organized initial records of arrest maintained at police stations, such as "police blotters" and "incident reports," if such records are not indexed or accessed by name and if they are permitted by law or longstanding custom to be made public;

(b) court record systems accessible only by date or by docket or file number, if comprised of records of public criminal proceedings that are open to public access, court opinions, including published compilations thereof, or records or indexes of pardons or paroles;

(c) records of traffic offenses maintained only for the purpose of regulating the issuance, suspension, revocation or renewal of drivers' licenses;

(d) records relating to violations of the Uniform Code of Military Justice maintained solely within the Department of Defense, and not disseminated to agencies or systems covered by the standards;

(e) statistical or analytical records or reports in which individuals are not identified and from which their identities cannot be ascertained;

(f) Identification record information; and

(g) Wanted person information.

Commentary

This Standard excludes from coverage criminal justice-related information that either does not represent a serious threat to personal privacy or should not be regulated as criminal justice information for reasons related to public policy.

For example, paragraph (a) of Standard 3.1 excludes various kinds of original records of entry that are maintained by criminal justice agencies on a chronological basis and that by law or well-established custom have been open to public inspection. An example is a police blotter, arrest book or equivalent record system maintained chronologically at police stations to record arrests. A primary function of such records is to provide current information to the press and the public about police activities, both to enable the press to report upon such activities and to guard against secret arrests. Because of the public policy served by the availability of such records, and because their chronological organization makes retrieval difficult and therefore less of a threat to an unwarranted invasion of privacy, the Standards recommend that such records continue to be open to the public. Where these records are retrievable by a name search, however, they would not be excluded.

Paragraph (b) concerns public court records and indexes of pardons or paroles accessible other than by name. As is the case with respect to original records entry, a key feature is that, in order to be excluded, such records must not be retrievable by a name search. For example, although chronologically arranged court case files may be made available to the public, any such files arranged and accessible by name may not be made available. Thus, if an index of case files is maintained that would enable an interested person to find and access all previous court case files relating to a specific individual, that index would remove the files from the exclusion of paragraph (b).

Paragraph (c) excludes traffic offense records maintained for noncriminal justice purposes, such as records maintained by state departments of motor vehicles for the purpose of administration of drivers' licensing laws.

Paragraph (d) excludes records of military offenses if such records are kept strictly within the military and are not linked to nonmilitary databases. The Uniform Code of Military Justice includes a comprehensive and separate set of standards for military justice information. Legislation concerning civilian criminal justice information invariably excludes military offense records.

The Standard in 3.1(e) would exclude statistical and analytical information in which individuals are not identified and from which their identities cannot be ascertained. Where criminal justice information cannot be connected with a specific individual, the content of the data and its method of organization are such that the information poses little threat to personal privacy.

Paragraphs 3(f) and (g) exclude identification record information and wanted person information, respectively. Identification record information is defined in Standard 2.1(g) expressly to exclude any suggestion that the individual has been suspected of or charged with a crime. Inasmuch as this type of record does not carry any stigma, there is no reason to apply the maintenance, use and dissemination safeguards in the standards. Wanted

person information, on the other hand, exists for the very purpose of indicating that the record subject has been charged with a crime; therefore, inasmuch as wanted person information is, by definition, public domain data, there is no reason to apply dissemination safeguards.

3.2. Criminal justice agencies are not restricted from continuing to disclose to the public and the press factual information about investigations, arrests and other criminal justice events if such disclosures are reasonably contemporaneous with the events, nor from responding to specific inquiries by the public or press about arrest records or criminal records of specific individuals if such responses are based on information described in paragraphs (a), (b) or (g) of Standard 3.1.

Commentary

Standard 3.2 reflects the existence of a strong public policy interest in permitting public disclosure of timely information relating to ongoing developments in criminal cases. Thus, this Standard would permit criminal justice agencies to respond to press or public inquiries that are specific as to particular events, as opposed to inquiries that seek full or partial criminal histories of named individuals. Thus, if a reporter were to ask whether a particular individual was arrested on a particular date, a criminal justice official could respond to that question if the response is based on data available to the public under Standard 3.1.

This Standard also ensures that, even in the absence of specific inquiries, announcements of ongoing criminal justice proceedings should be permitted if such announcements are "reasonably contemporaneous" with the event to which they relate. Thus, criminal justice agencies may make press statements concerning such events as new developments in investigations, arrests, convictions or incarcerations, so long as the announcements occur within a relatively short period following the event during which it would be considered newsworthy. In most cases, this period would be no longer than a week, although there conceivably are situations, such as cases involving celebrated individuals, in which the period may be longer.

Standard 4. Correctional and Release Information

Correctional and release information shall be available only to:

(a) criminal justice agencies for criminal justice purposes and to the extent necessary for the performance of duty; or

(b) the record subject or his attorney if authorized by federal or state statute or regulation or court order or rule.[22]

Commentary

Correctional and release information should be available for dissemination to, and use by, criminal justice agencies for any authorized purposes related to the performance of their duties. The Standard provides, however, that such information should not be disseminated to noncriminal justice agencies.

Correctional and release information can include extremely sensitive subjective and normative data that, if disclosed, may damage the subject. In view of the sensitivity of correctional and release information and the limited degree of its potential utility to the public or to private sector organizations, disclosure cannot be justified except to recipients, such as criminal justice officials, who can make particularly persuasive claims for access.

This Standard also recognizes that there exists a substantial body of statutory and regulatory law regarding access by record subjects and their attorneys to correctional and release data. In general, this law permits access to correctional and release record information, particularly in situations where the information has been used to make a material decision about the record subject, such as parole.[23] This body of law also recognizes exceptions to the right of access where such access would pose a threat of harm to third parties or would impair a treatment relationship or a confidential relationship or in certain other circumstances.[24] Standard 4(b) defers to this law by providing that a record subject or his attorney have access to correctional and release data *only* if authorized by applicable federal or state law.

---

[22] To the extent possible, this is a gender-neutral document. In those few circumstances when the masculine gender is used, it is deemed to be a reference to both masculine and feminine genders.

[23] *Paine v. Baker*, 595 F. 2d 197 (4th Circ. 1979), *cert. denied* 444 U.S. 925 (1979); *Coralluzzo v. New York State Parole Board*, 566 F. 2d 375 (2d Cir. 1977), *dismissed after cert. granted* 435 U.S. 912 (1978).

[24] See, e.g., Massachusetts, Department of Correction, *Regulations Governing Access to and Dissemination of Executive Information*, 103 CMR 157.

Standard 5. Segregation of Intelligence and Investigative Information

Criminal intelligence and investigative information shall be physically or logically segregated from other types of criminal justice information, and, when such other types of criminal justice information is disseminated, shall not contain any information that would indicate or suggest that a criminal intelligence or investigative file exists on the individuals to whom the information relates.

Other types of criminal justice information may be included in criminal intelligence and investigative files, but shall not, solely by reason of such inclusion, become subject to the restrictions on access and dissemination applicable to criminal intelligence and investigative information.

Commentary

In view of the sensitive nature of much intelligence and investigative information, and particularly in view of the fact that such information often is unverified, this Standard provides that intelligence and investigative information be physically or logically segregated from other types of criminal justice information. Other types of criminal justice information are based upon verified occurrences and thus are far more factually reliable.

In order to discourage the linkage of intelligence and investigative information and other types of criminal justice information, it is recommended that criminal justice information not include any reference to whether an intelligence or investigative file exists with respect to a particular individual. In view of the fact that other types of criminal justice information are often used to make administrative decisions about record subjects, it is especially appropriate that intelligence and investigative information — which is used primarily for leads and seldom used to make dispositive decisions about record subjects — is segregated. Since the Standards apply more restrictive dissemination safeguards to intelligence and investigative data than they do to other types of criminal justice information, there is no need to prohibit the inclusion of other types of criminal justice information in intelligence and investigative files.

The term "physically segregated" means that intelligence and investigative information should be maintained in a manual system or an automated database that is physically distinct and separate from systems or databases which contain other kinds of criminal justice data, such as criminal history data. Alternatively, the Standard permits intelligence and investigative data to be logically segregated from other types of justice data. The term "logically segregated" means that intelligence and investigative data can be kept in a system or database with other types of criminal justice data, provided that the system has the capability, through system architecture, software or otherwise, to segregate intelligence and investigative data from other types of criminal justice data. Moreover, when other types of criminal justice data are disseminated, they must not indicate that an intelligence or investigative record exists.

Standard 6. Direct Access to Criminal Justice Information

6.1. Direct access to criminal justice information systems should be limited to authorized officers or employees of criminal justice agencies, except as provided in Standard 6.2. Each agency should have operating procedures to restrict access to criminal justice information to those officers and employees who are authorized to have particular kinds of information; who need such information for the performance of their duties; who will use such information for authorized purposes only; and who will not redisclose such information to recipients who are not eligible under the Standards to receive the information.

6.2. Agencies of the federal government authorized by federal statute to conduct investigations determining the eligibility for security clearances allowing access to classified information or for appointment to or retention in national security duties may, at the discretion of a criminal justice agency, be permitted direct terminal access to a criminal history record information system for such national security checks.

Terminal access shall be subject to an agreement between the criminal justice agency and the federal agency which protects the interests of the criminal justice agency and record subjects, and which includes provisions for positive identification and audit. Criminal justice agencies which provide direct terminal access to such federal agencies are authorized to charge the federal agency for all costs associated with such direct access.

Commentary

Standard 6.1 provides that authorized officers or employees of a criminal justice agency may be given direct

access to a criminal justice information system. The term "direct access" is not defined in the Standards. This term is defined in the Justice Department Regulations to mean "having the authority to access the criminal history record database, whether by manual or automated methods."[25] This, however, is not the way in which the term "direct access" is used in the Standards. The term is used in these Standards to mean access to information in an information system, whether by automated or manual means, by an individual or agency without intervention by or the assistance of any other party or agency.

Security is sometimes defined as the ability of a record manager to keep his promises about confidentiality. In this sense, direct access always poses a threat to security because it strips record managers of access control. Accordingly, it is important that the circumstances under which direct access is permitted are limited and that appropriate safeguards are attached.

For this reason, Standard 6.1 attaches four conditions to direct access by criminal justice officials: (1) only employees with legal authority for direct access are permitted to have direct access; (2) authorized employees must have a need for direct access; (3) employees with direct access must use the information only for authorized purposes; and (4) employees with direct access must not redisclose the information obtained through direct access to individuals who are not eligible under the Standards to receive such information.

It is contemplated that agencies will express these safeguards in writing by specifically identifying those employees who have direct access; by setting forth the circumstances under which authorized employees have a need for direct access; and by either entering into agreements with applicable employees to the effect that they will comply with the safeguards or by expressing these safeguards as conditions of employment in employee manuals or other appropriate documents.

Standard 6.2 is a response to the Security Clearance Information Act (SCIA). The SCIA requires state and local criminal justice agencies, upon request, to make available criminal history record information to designated federal agencies for background investigations for eligibility for security clearances or appointment to or retention in national security duties. However, the SCIA does not require state and local agencies to give SCIA agencies direct access to their information systems. As a consequence of the passage of this law, the volume of federal "national security" requests to state and local agencies is expected to increase significantly. For this reason, or for other reasons, some state and local agencies may wish to give SCIA agencies direct access to their criminal history record systems, and Standard 6.2 reflects this possibility.

If, however, direct access is provided to federal agencies, these agencies are expected to enter into written agreements with the state or local agency operating the information system. The agreement should incorporate the personnel safeguards in Standard 6.1, as well as any other safeguards, such as the security safeguards in Standard 11, which the criminal justice agency determines are necessary in order to protect the interests of the agency and record subjects. In addition, and at a minimum, these safeguards must include a provision for positive identification, consistent with Standard 10, and for auditing, consistent with Standard 18.

Of necessity, this Standard contemplates that direct access may involve a name-only search as a basis for initial access to a record, to be followed by verification by a technical search relying upon fingerprints. The technical search must be completed prior to the SCIA agency's use of the record as a basis for any decision about the record subject.

Finally, criminal justice agencies are specifically authorized by the SCIA to charge federal noncriminal justice agencies for all reasonable costs associated with providing direct access, provided that the amount charged does not exceed the charges to state or local noncriminal justice agencies. Such charges can include the capital costs associated with acquisition and installation of appropriate equipment; initial and ongoing manpower costs; and *pro rata* overhead costs. Of course, criminal justice agencies retain discretion to provide access without charge whether pursuant to III protocols or otherwise.

Standard 7. Use of Criminal Justice Information By Criminal Justice Agencies

Criminal justice information shall be permitted to be used by government agencies and criminal justice agencies for criminal justice employment purposes and by criminal justice agencies for other criminal justice purposes under agency rules or regulations specifically designed to limit such use to the following purposes:

(a) the commencement of prosecution, determination of pretrial or post-trial release or detention, the adjudication of criminal proceedings or the prepa-

[25] 28 C.F.R. § 20.3(1).

ration of a presentence report;

(b) supervision by a criminal justice agency of an individual who has been committed to the custody of that agency prior to the time the arrest occurred or the charge was filed;

(c) the investigation of an individual when that individual has already been arrested or detained;

(d) the development of investigative leads for particular criminal offenses if access to the information is limited to criminal justice officials with both a need and a right to have access to such information;

(e) the alerting of an official or employee of a criminal justice agency that a particular individual may present a danger to his safety or for similar essential purposes; or

(f) such other legitimate criminal justice purposes as are set forth in agency rules or regulations.

Commentary

The basic purpose of this Standard is to identify, in some detail, the breadth of permissible uses of criminal justice information by criminal justice agencies, and to require criminal justice agencies to give thought to their policies for the use of such information by requiring these agencies to adopt rules or regulations. This Standard reflects the view that the characteristics of criminal justice agencies and the purposes for which they use criminal justice information justify the most liberal Standards for their access to and use of such information. Criminal justice information is, after all, principally collected and maintained to assist criminal justice agencies to perform their vital missions. If criminal justice agencies cannot freely obtain access to criminal justice information, their ability to accomplish their missions is likely to be compromised. Further, published research, as well as testimony at Congressional hearings, indicates that criminal justice agencies generally use criminal justice information in a responsible manner. According to these sources, the vast majority of instances of information abuse and subject injury occur after criminal justice information leaves the criminal justice community.[26]

Accordingly, this Standard requires that criminal justice agencies be permitted access to and use of criminal justice information for all legitimate criminal justice purposes, such as investigation, prosecution, adjudication and detention.

In addition, the Standard requires that criminal justice information be available for criminal justice employment purposes. The Standard gives criminal justice agencies access for employment screening purposes and also gives the President, governors, mayors, other executive branch officials and legislative officials, access to criminal justice information for determinations about appointments of judges, police commissioners and other police executives. It is not contemplated, however, that executive branch agencies would have direct access for such purposes, but rather would be required to submit requests through a criminal justice agency.

Employment screening for criminal justice purposes is judged to be a critical use. Without such access, the public would run a significant risk that individuals charged with criminal justice responsibilities would have a history of involvement with the criminal justice system. This result might seriously compromise the criminal justice system's ability to accomplish its mission, while doing significant damage to public confidence in criminal justice officials.

Finally, since the purpose of this Standard is not to restrict the use of criminal justice information within the criminal justice community, the Standard contains a "safety valve" provision in paragraph (f) to permit "such other legitimate criminal justice purposes as are set forth in agency rules or regulations."

Standard 8. Access by Individuals for Purposes of Challenge

8.1.

(a) Any individual who satisfactorily verifies his identity and complies with reasonable rules and regulations shall be permitted, in person or through counsel, to review and obtain a copy of any criminal history record information or criminal index information concerning him maintained by

---

26 A. Hess and F. LePoole, "Abuse of the Record of Arrest Not Leading to Conviction," *Crime and Delinquency* 13 (1969) : 494-505; see also Testimony of Rocky Pomerance, Police Chief, Miami Beach, and President, International Association of Chiefs of Police, at U.S., Congress, Senate, Committee on the Judiciary, *Hearings Before the Subcommittee on Constitutional Rights of the Committee on the Judiciary on S.2008*, 94th Cong., 1st sess., 1975, p. 149.

the criminal justice agency receiving the individual's access request, for the purpose of challenging its accuracy or completeness or the legality of its maintenance.

(b) Each criminal justice agency shall adopt and publish rules and procedures to implement this section, including some method of administrative review of any challenge the individual may make and some method of ensuring that appropriate corrections are made and that appropriate notice of such corrections is given to criminal justice agencies that have received inaccurate or incomplete information.

(c) Each state shall provide a procedure for administrative appeal upon request by the individual in instances in which a criminal justice agency refuses to correct challenged information to the satisfaction of the individual. In appropriate cases, such appeal shall include a hearing at which the individual shall be permitted to appear, with or without counsel, to present evidence and to examine and cross-examine witnesses.

(d) Each state shall provide for judicial review of any final decision taken after administrative appeal pursuant to paragraph (c) if the individual is not satisfied with such decision and of any failure to provide to any individual any right set out in this Standard.

Commentary

Paragraph (a) of this Standard provides individuals who are the subject of arrest or conviction records with a right to obtain a copy of the record or any supporting index information maintained by the agency receiving the request, and to challenge its legality, accuracy or completeness. In paragraph (b) the Standard requires criminal justice agencies to establish an administrative review procedure to be used when recordkeepers and subjects disagree about the inclusion in the record of a subject's proposed corrections. In addition, paragraph (b) would require agencies to ensure that when corrections are made, other criminal justice agencies which have previously received the incorrect record receive notice of the corrections. Paragraphs (c) and (d) call upon the states to establish administrative and judicial appeal mechanisms.

This Standard recognizes that access should not be permitted where the access will sabotage an ongoing investigation (intelligence and investigative information) or limit the candor and subjectivity of normative records (correctional and release information). Thus, the Standard permits access only to criminal history record information and wanted person information.

Subject access to criminal history records is fundamental to basic fairness. Subject access also tends to improve the accuracy and completeness of records in an information system. Furthermore, subject access helps to quiet fears of government surveillance. For all of these reasons, subject access provisions are included in virtually every state statute and the Justice Department Regulations. The Justice Department Regulations require agencies to implement a subject access Standard that is very similar to the provisions in this Standard. The Department's Regulations differ in only two respects: (1) review and appeal procedures are not as complete; and (2) the Regulations do not specifically permit the subject to authorize his lawyer to obtain access.

Paragraph (b) of this Standard requires recordkeepers to ensure that other criminal justice agencies that have received a record are notified of corrections or changes. This requirement must be read in conjunction with Standard 12 for accuracy and completeness which requires that a log be maintained describing each dissemination that has occurred within the prior three years. Accordingly, correction notifications are not required beyond a three-year period. Also, agencies are given discretion in implementing this requirement, in that only "appropriate" notices of corrections are required. Thus, where the nature of the correction is not significant, notice need not be provided. Similarly, if notice would impose an onerous burden on the agency, or is otherwise inappropriate, it may be avoided.

The administrative appeal provisions in paragraph (c) require states to provide record subjects with extensive due process protections. Because the approach in paragraph (c) is ambitious, it is recognized that states should be accorded substantial latitude in interpreting and applying the safeguards in paragraph (c).

8.2. No individual who obtains any copy of any information regarding himself under this Standard may be requested or required to transfer or show such copy to any other person or agency, and any request for such a transfer or disclosure shall be prohibited.

Commentary

This Standard reflects the view that requesters should obtain criminal history record information from criminal justice agencies directly and not indirectly from record subjects. Obtaining information from record subjects substantially increases the risk that partial or out-of-date information will be obtained. Such a practice also runs the risk, in some circumstances, that a private party who is not authorized access to a record will obtain access by applying pressure upon the record subject.

Standard 9. Maintenance, Dissemination and Use of Criminal Intelligence and Investigative Information

(a) Criminal intelligence and investigative files shall be reviewed at regular intervals — and, at a minimum, upon any request for dissemination of particular information — to determine if the grounds for retaining the information still exist and, if not, it shall be destroyed.

(b) Within a criminal justice agency, access to and use of criminal intelligence and investigative information shall be strictly limited to officers and employees who are authorized to have such access and use and who have a demonstrable need for particular information.

(c) Criminal intelligence and investigative information shall be disseminated outside of the collecting agency only for the following purposes:

(1) confirmation of information in the files of another criminal justice agency; or

(2) for criminal justice employment or other criminal justice purposes, such as an investigation of an individual by another criminal justice agency, if the requesting agency gives assurance that the information is relevant to the criminal justice purpose.

(d) An assessment of criminal intelligence and investigative information may be provided to a governmental official or to any other individual when necessary to avoid imminent danger to life or property.

Commentary

Paragraph (a) provides that intelligence and investigative information cannot be retained indefinitely in individually indexed files in the absence of a reasonable basis for determining that the information is relevant to known or suspected criminal activity. Thus, intelligence and investigative files must be reviewed at regular intervals — the frequency depending upon such factors as the potentially damaging nature of the information and whether or not the information system is automated — to determine if its further retention can be justified. For example, if an agency is maintaining intelligence or investigative information of questionable reliability or relevance, and subsequent investigation does not develop supporting information, the information in question should be destroyed within a reasonable period. Moreover, even when intelligence or investigative information provides a reasonable basis for believing that the record subject is involved in criminal activity, the information in question should be reviewed regularly. At a minimum, a review must be conducted whenever a request for dissemination of the information in question is received.

The principal reason for this safeguard is that intelligence and investigative files, by their very nature, contain raw and unverified information. A typical intelligence file is likely to contain at least some of the following kinds of information about suspects: name, address, aliases, nicknames, Social Security number, date and place of birth, marital status, name of spouse, race, physical description, criminal history record, motor vehicle record, names and addresses of business associates, parental background, educational background, military background, employment history, affiliation with organizations and groups, financial and credit status, habits and traits, places frequented, past activities, and other police findings and observations. An investigative file is likely to contain some, although usually not all, of the same information. Customarily, an investigative file will also contain more detailed physical descriptions and less information about background and associates (since the suspect's identity is often unknown, which is less often the case in intelligence investigations).

Paragraph (b) of this Standard provides that intelligence and investigative information should be available within the criminal justice agency maintaining the information only to authorized employees on a "need-to-know" basis. In general, this means that a criminal justice official requesting access to an intelligence or investigative file must establish that he is conducting an investigation pursuant to his official duties and that he needs the information in connection with the investiga-

tion. In view of the size and diverse nature of many criminal justice agencies, strict limitations on intra-agency sharing of information is an important safeguard.

Paragraph (c) sets out the circumstances under which intelligence and investigative information must be disseminated outside of the agency that maintains the information. Historically, intelligence and investigative data have not been available except within the criminal justice community, and sometimes not even within that community. Under paragraph (c), dissemination of intelligence and investigative information must be limited to criminal justice agencies for valid criminal justice purposes, such as for confirmation of information which the requester already has or for investigative purposes, based upon legally valid grounds.

Statutes in several states affirmatively prohibit the disclosure of intelligence and investigative data, except to other criminal justice or law enforcement agencies. In addition, the tort doctrines of defamation and invasion of privacy can, at least in some circumstances, lead to liability of criminal justice agencies and their officers for disclosure of intelligence and investigative data. Moreover, release of these data may violate record subjects' constitutional rights of due process, or perhaps privacy, if the data are inaccurate or incomplete, and if release results in some tangible harm to the record subject.

Paragraph (d) permits criminal justice agencies, in their sole discretion, to provide an "assessment" of intelligence or investigative information to a government official or other individual where necessary to avoid an imminent danger to life or property. For example, this paragraph permits a disclosure of intelligence or investigative information to national security agencies in emergency circumstances where a threat to life or property is involved. This paragraph, however, is not authority for the release of intelligence and investigative information for purposes of national security background investigations.

This paragraph contemplates that actual intelligence or investigative records would not be released, but rather, only an oral excerpt or summary or, in unusual circumstances, a written excerpt or summary.

Standard 10. Positive Identification of Record Subjects

10.1. Except as permitted in Standard 10.2, criminal justice information, except criminal intelligence and investigative information, shall be available only on the basis of positive identification of an individual by means of fingerprints or other equally reliable means.

10.2. A criminal justice agency shall be permitted to respond to requests for criminal justice information from criminal justice agencies, and from noncriminal justice agencies for national security purposes consistent with the Security Clearance Information Act, based upon name, date of birth, sex and/or other identifiers, other than fingerprints, where necessary for criminal justice or national security purposes, and provided that the record prominently indicates that it has not been furnished on the basis of positive identification.

Commentary

Standard 10.1 establishes a general rule that criminal justice information, except criminal intelligence and investigative information, shall be available only on the basis of positive identification by means of fingerprints or other equally reliable means. "Other equally reliable means" include biometric identification processes, such as DNA typing, that result in the positive identification of an individual. This Standard contemplates that an agency could initially conduct a name-only search and then follow up that search with a fingerprint or similar verification or, alternatively, an agency could conduct an initial search (technical search) on the basis of fingerprints or other means of positive identification.

Name-only searches that are not supported by positive identification can result in significant problems. For instance, individuals may be misidentified and, consequently, criminal justice information may be disseminated about the wrong individual. In addition, name-only searches often fail to result in the identification of relevant records about the subject of the search. For example, studies of the FBI's responses to name-only searches requested by federal noncriminal justice agencies indicate that the productivity of the search — e.g., the likelihood that the search will produce a "hit" — declines substantially when the search is conducted on a name-only basis, as opposed to being conducted on the basis of fingerprints.

The development of new positive identification technologies, such as automated fingerprint identification systems, makes it far more cost-effective to confirm this made on the basis of name-only information or, for that matter, to conduct initial searches using either rolled or latent fingerprints. These advanced technologies are also tolerant of poor quality prints. As a consequence, it is far easier today than ever before to obtain a positive identification on the basis of fingerprints.

Standard 10.2 permits criminal justice agencies to respond to requests based upon name, date of birth, sex or other identifiers, other than fingerprints, if the requests

April 24, 1989

FEIN #94-2247019

Alice Liu
National Institute of Justice/NCJRS
Acquisition Report Department
Box 6000
Rockville, MD 20850

INVOICE

Enclosed is the material you requested. Please make your check payable to SEARCH Group, Inc. for the total amount due shown below.

Publication Technical Report #13

Printing/Reproduction Costs $_____

Postage/Handling $_____

California State Sales Tax $_____

TOTAL AMOUNT DUE $ N/C

SEARCH Group, Inc.
The National Consortium for Justice Information and Statistics
925 Secret River Drive, Suite H / Sacramento, California 95831
(916) 392-2550

are made by criminal justice agencies or by federal agencies, consistent with the terms of the Security Clearance Information Act. Under the terms of Standard 10, however, noncriminal justice and non-SCIA requests could be processed only on the basis of positive identification.

Criminal justice agencies are often required to make name-only requests because they often will not have a suspect's prints. Also, in many instances, criminal justice agencies must obtain the results of their search quickly and therefore cannot wait for the repository or other agency conducting the search to receive the prints. Advances in facsimile transmission capabilities for fingerprints may reduce the extent to which time pressures force criminal justice agents to rely upon the results of name-only searches.

Paragraph 10.2 also permits criminal justice agencies to respond to name-only requests by federal agencies where the criminal justice agency is required to do so under the SCIA. Under the SCIA, state and local criminal justice agencies are required to respond to otherwise valid name-only requests by SCIA agencies unless the state agency is a central state repository which uses fingerprints in an automated fingerprint identification system and an applicable state law requires the submission of fingerprints. Only in that relatively narrow circumstance may SCIA agencies be required to submit prints. The legislative history of the SCIA, however, indicates that federal agencies should also submit prints to any state or local criminal justice agency when necessary to prevent a misidentification of a record subject. Presumably, this is a reference to instances where the name-only search produces several hits, and it is not possible on the basis of nonfingerprint information to make a determination as to which record is responsive to the request. In all other instances, agencies covered by the SCIA can require state and local criminal justice agencies to process their requests on a name-only basis. Accordingly, Standard 10.2 recognizes this federal requirement.

Standard 10.2, however, also requires that whenever criminal justice information is made available on the basis of a name-only check, whether to criminal justice agencies or to federal national security agencies, the record must prominently indicate that it has not been furnished on the basis of positive identification. This requirement contemplates that an appropriate legend will be stamped or otherwise permanently and prominently affixed to the rap sheet or other criminal justice record. A legend of this kind protects both users and record subjects.

It should also be noted that the direct access authorization in Standard 6 is not an exception to the positive identification requirements of this Standard. Thus, information provided through direct access must still be made available only on the basis of positive identification, except that it is contemplated that requesters authorized to have direct terminal access under Standard 6.2 can obtain records on the basis of a name-only check, and thereafter, "hits" must be verified by a fingerprint comparison or other means of positive identification. The technical verification must be completed before the criminal justice information is used as a basis for a decision about a record subject.

Standard 11. Security

Each criminal justice agency shall adopt operational procedures reasonably designed to:

- **(a) ensure the physical security of criminal justice information in its custody and to prevent the unauthorized disclosure of such information;**
- **(b) ensure that when criminal justice information is stored in an automated system, effective and technologically advanced software and hardware designs are instituted to prevent unauthorized access to such information;**
- **(c) ensure that communications lines, whether dedicated or shared, over which criminal justice information is transmitted, are operated so as to detect and prevent unauthorized inquiries, record updates, destruction of records or unauthorized access or tampering;**
- **(d) ensure that central repositories are protected from unauthorized access, theft, sabotage, fire, flood, wind or other natural or man-made disasters, and that adequate backup facilities are available so that, in the event that criminal justice information maintained in such repositories is destroyed or damaged, copies of such information are readily available at a backup site; and**
- **(e) ensure that personnel security procedures are employed, including appropriate background investigations, and that the agency has authority to transfer or remove personnel who are judged to be security threats.**

Commentary

The security of information in manual and automated

criminal justice information systems has been one of SEARCH's primary concerns since its founding. Project SEARCH's *Technical Report No. 2*, published in July 1970, devotes an entire chapter to system security. The definition of "security" that is found in *Technical Report No. 2* is still valid:

> [Security 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.[27]

In point of fact, security is a prerequisite for any information system. Maintenance of information in an insecure environment destroys the recordkeeper's ability to control the system and permits the entry of erroneous information, the destruction of appropriate information, and the unauthorized dissemination of information. Security is a special concern in systems which maintain criminal justice information. Unauthorized access to and use of criminal justice data can cause severe harm to record subjects. Furthermore, unauthorized access can jeopardize numerous criminal justice interests, including, in particular, investigative interests.

The extent and nature of security safeguards that ought to be implemented in criminal justice information systems has prompted considerable debate. Nevertheless, there is wide agreement that basic security plans are needed in any criminal justice information system. The Federal Crime Control Act of 1973 and the Justice Department Regulations require the adoption of security safeguards in criminal justice information systems. The Senate Report on the Crime Control Act of 1973 recommended that the Justice Department Regulations track the security Standards found in *Technical Report No. 2*. Not surprisingly, the security provisions in Standard 11 also track SEARCH's original security Standards published in *Technical Report No. 2*. Although Standard 11 is relatively detailed, it assumes, like most of the Standards, that individual criminal justice agencies will develop their own implementation strategies to comply with the Standard.

Paragraph (a) requires each criminal justice agency to establish procedures reasonably designed to ensure the physical security of criminal justice information in its custody and thereby to prevent unauthorized access to such information. While each agency is free to develop its own physical security procedures, the types of procedures which are contemplated include:

- the establishment of physical barriers, sign-in procedures and guards, and the use of badges, keys or technological locking devices;
- the segregation of terminals and files and other physical locations where information is used and displayed so that visual surveillance or eavesdropping is discouraged; and
- procedures for escorting visitors, maintenance personnel and equipment vendors.

Paragraph (b) requires that when criminal justice information is stored in an automated system, effective and technologically advanced software and hardware designs are instituted to prevent unauthorized access to the information. Importantly, paragraph (b) does not require that agencies use only "dedicated" computer systems — that is, equipment that is set aside exclusively for the use of the criminal justice information system. Although the dedication of equipment to a criminal justice information purpose is an effective means of promoting security, advances in hardware and software security permit an appropriate level of security to be achieved even when a system is not dedicated.

The types of procedures that could be characterized as reasonably designed to ensure security in an automated system will vary greatly depending upon the exact use and location of the system; the type of hardware and software in place; other elements of system architecture; and the presence of related security safeguards, such as physical and personnel security. The types of safeguards that can contribute to automated security include the following:

- the use of identification code numbers or passwords for each terminal and user;
- an automated log of all inquiries, authorized or unauthorized, and all disseminations;
- software which specifies the use that can be made of each terminal;
- procedures to allow for the suspension of remote terminal access in suspicious situations;
- software which is programmed to alert system managers of unauthorized requests;
- programs that prohibit inquiry, record updates or destruction of records from terminals that are not authorized; and
- secrecy for key software programs.

Paragraph (c) requires the adoption of operational

---

[27] Project SEARCH, California Crime Technological Research Foundation, *Security and Privacy Considerations in Criminal History Information Systems*, Technical Report No. 2 (Sacramento, CA: California Office of State Printing, July 1970), p. 39.

procedures reasonably designed to assure that communication lines over which criminal justice information is transmitted are operated so as to detect and prevent unauthorized inquiries, record updates, destruction of records or unauthorized access or tampering. This Standard is particularly important in view of the direct access permitted for criminal justice agencies and, in certain circumstances, noncriminal justice, national security agencies under Standard 6. The types of procedures reasonably designed to secure communication lines are the same types of procedures that can be used to ensure security in automated information systems.

Paragraph (c) does not contemplate that criminal justice information transmitted over communication lines must be scrambled or coded. It is believed that there are adequate security procedures currently available to discourage eavesdropping, tapping, insertion of false messages or other types of tampering with communication lines without the need to scramble messages.

Paragraph (d) requires the implementation of operational procedures reasonably designed to ensure that central repositories are protected from unauthorized access, theft or other natural or manmade disasters, and that adequate backup facilities are available so that copies of criminal justice information are readily available at backup sites in the event of a disaster. The specific types of procedures to be implemented to protect central repositories against natural or manmade disasters and to provide for backup are left to each agency. In general, such procedures can include the following:

- specific site configuration safeguards to assure against fire, flood, theft and other natural or manmade disasters;
- adequate fire detection and suppression devices;
- use of fireproof and lockable filing cabinets;
- environmental monitors and controls for temperature, humidity, etc.; and
- an emergency shutdown procedure of the information system and all of its power sources.

With respect to the establishment of backup facilities, it is contemplated that repositories will maintain a full set of duplicate files at an off-premises site. Care should be taken for proper labeling of information at the backup site and proper environmental control to permit long-term storage of such data.

Paragraph (e) requires the implementation of operational procedures that are reasonably designed to ensure that personnel security procedures are employed, including appropriate background investigations, and that the agency has authority to transfer or remove personnel who are judged to be security threats. The types of personnel security procedures to be employed are left to each agency, but it is contemplated that they may include the following:

- an identification of all personnel who need to have access to a criminal justice information system;
- identification of the types of records to which each employee should have access;
- a personal interview with each employee who is authorized access and periodic reinterviews;
- a national records check to determine if an applicant has a criminal history record and periodic rechecks of employees.

Standard 12. Accuracy and Completeness

12.1. Each criminal justice agency shall maintain criminal history record information in such a manner as to ensure that the criminal history record information is accurate and complete, and shall adopt the following policies and procedures, which are reasonably calculated to produce the highest quality of criminal history record information:

(a) ensure that disposition and other additional or corrective information pertinent to original arrest records are promptly reported for inclusion on such records;

(b) ensure that records are made and maintained, for a period of at least three years, of —

(1) the source of arrest record information and criminal offender record information; and

(2) the identity of other agencies or persons to whom criminal history record information is disseminated, together with the date of the dissemination, the authority of the requester, the purpose of the request, and the nature of any information provided;

(c) ensure that information and formats are standardized for reporting and entering information into criminal history record systems throughout the state;

(d) ensure that procedures are in place to systematically and in detail review and verify entries in criminal history records;

(e) ensure that a tracking and linking system is used to match disposition

entries with charge entries and to match other types of subsequent entries with original entries;

(f) ensure that a disposition monitoring system has been implemented which flags aged arrest entries and provides for procedures to obtain dispositions for these entries;

(g) ensure that there is a regular program of auditing;

(h) ensure that the central repository is queried prior to making criminal history record information available, unless the information in question was originated by the disseminating agency or the agency knows that the central repository does not maintain such information or the central repository is incapable of responding within the necessary time period;

(i) whenever possible, implement automated systems which include data quality protocols of the type identified in this Standard;

(j) implement policies and procedures which promote and facilitate communication with the courts and other parts of the criminal justice system in order to maximize the sharing of disposition and other relevant information; and

(k) ensure that a criminal history record information sheet ("rap sheet") clearly indicates the linkages among arrest, charge and disposition information and bears a conspicuous legend which states the date on which the rap sheet is issued and a warning that the rap sheet information is current only as of the date of issuance.

12.2. A state may exempt from compliance with this Standard information entered into information systems prior to the adoption date of the Standards.

Commentary

The accuracy and completeness of criminal history record information is one of the most, if not the most, significant information issues confronting the criminal justice community. Accordingly, this Standard requires that each criminal justice agency maintain criminal history record information in such a manner as to ensure that the criminal history information is accurate and complete. No numeric requirement is imposed since it is understood that the goal should always be to maintain all information in a manner that is accurate and complete. The Standard identifies 11 policies and procedures which have been demonstrated to improve the quality of criminal history record information and requires that agencies implement these procedures. The Standard, however, contemplates that in some cases, an agency may properly determine that it is impractical or inappropriate to implement a particular procedure.

Criminal history record information is vital at virtually every stage in the criminal justice process. From an initial arrest to a final decision to release, criminal history record information plays a significant role. Unfortunately, the available research indicates that the accuracy and completeness of criminal history record information in at least some central repositories, and particularly in local criminal justice systems, is deficient, especially with regard to court dispositions. Studies by the U. S. Congress' Office of Technology Assessment indicate that, as a national average, the state central repositories have achieved approximately a 65 percent disposition reporting rate.[28] This rate, however, varies significantly from state to state and varies further with respect to the age of the records being sampled. Relatively recent entries tend to have significantly higher accuracy and completeness rates. Studies by OTA and others indicate that the FBI's criminal history system has an even lower disposition reporting rate.[29]

In states that have enjoyed success in improving the accuracy and completeness of their criminal history records, research indicates that they have implemented many, if not all, of the safeguards and procedures set forth in paragraphs (a) through (k). Paragraph (a) requires agencies to implement a system to assure that disposition and other information pertinent to original arrest records are promptly reported for inclusion on such records. Although many state statutes require the prompt reporting of information to repositories and other criminal justice agencies, research suggests that agencies maintaining these records must implement their own followup and monitoring procedures if they are to be confident that mandated reporting will take place. Of course, in many states, statutory relief is necessary in order to assure proper reporting and proper followup and

---

28 See note 6, pp. 93-94.

29 Ibid., pp. 91-92.

monitoring.

Paragraph (b) requires that a transaction log be maintained which describes the source agency for each arrest record entry and which identifies agencies or persons to whom information is disseminated, together with the date of the dissemination, the authority for the dissemination, the purpose of the dissemination, and the nature of any information provided. Transaction log records must be maintained for three years. Most state statutes require transaction logs of this type. A transaction log requirement of this type not only facilitates audits of the system, but also permits criminal justice agencies to notify record recipients of any errors or corrections, including those brought to their attention by criminal record subjects.

Paragraph (c) requires that information and formats be standardized for reporting and entering information into information systems throughout the state. It has become something of a truism that uniform documentation promotes the collection of uniform data. Uniform data, of course, makes it far easier for agencies to verify data and to ensure that appropriate data have been received. Uniform reporting formats also encourage the reporting of data.

Paragraph (d) requires that procedures be in place to systematically review and verify entries in criminal history records. This Standard contemplates a system of edit-checking and verification that identifies and screens out questionable data prior to its entry into the system. In automated systems, this task is accomplished relatively easily. In manual systems, the task is more difficult, but still feasible and, if anything, even more important. It is contemplated that positive identification techniques are part of the review and verification process. Positive identification by means of fingerprints or other equally reliable biometric identification, is the only completely reliable way to ensure that incoming information is entered onto appropriate rap sheets and that agencies do not maintain multiple rap sheets about the same offender.

Paragraph (e) requires that a tracking and linking system be used to match disposition entries with appropriate charge entries. The inability of agencies to match disposition entries with charge entries is a surprisingly common problem. The reason that the problem is so widespread is that criminal history records may contain not only original arrest charges but also formal charges entered by a prosecutor; therefore, it is often difficult to match a subsequent disposition with the charge to which it pertains. Tracking and linking systems assign unique numbers to each charge, thereby making it possible to track a charge through the entire process. In so doing, not only is the rap sheet made more readable and reliable, but its utility for statistical purposes is enhanced. In particular, the utility of the records for Offender-Based Transaction Statistics (OBTS) research is increased.

Paragraph (f) requires the implementation of a disposition monitoring system which flags aged arrest entries and establishes procedures to obtain dispositions for these entries. Disposition monitoring systems are generally thought to be one of the most important techniques to improve data quality. The waiting period that must elapse before an arrest is cited as delinquent is left to each agency's discretion, but as a general matter, not less than three months is used as a waiting period.

Paragraph (g) requires that there be a regular program of auditing. The type of audit contemplated under the Standards is discussed in the commentary that accompanies Standard 18. Research has found that auditing is an indispensable tool for determining if information in a system is accurate and complete and for identifying specific steps that should be taken to cure any deficiencies.

Paragraph (h) requires that the central repository be queried prior to making criminal history record information available, unless the information in question was originated by the disseminating agency, or the agency knows that the central repository does not maintain the information, or the central repository is judged to be incapable of responding within the necessary time period. The Justice Department Regulations require agencies to establish procedures to query the central repository prior to disseminating criminal history information. In addition, numerous state statutes impose this same requirement. Given the mobility of criminal offenders and the differences in the accuracy and completeness of rap sheets maintained by state and local criminal justice agencies, it is critical that these agencies query the repository before disseminating criminal history record information.

Paragraph (i) requires that, where possible, agencies establish automated systems which include data quality safeguards of the type identified in this Standard. SEARCH's research has found that automation frequently is cited as a principal reason for an agency's improvement in the accuracy or completeness of its criminal history information. Automation is thought to contribute to data quality because it usually makes it easier and less expensive to implement data quality safeguards. Tracking and linking systems, editing systems, disposition monitoring systems and transaction logs, in particular, are more readily implemented and maintained in an automated environment.

Paragraph (j) requires that agencies implement policies and procedures which promote and facilitate communication with the courts and other parts of the crimi-

nal justice system. States which have implemented automatic systems, by which court dispositions are communicated from the courts to the repository, have found that their disposition reporting rate increases dramatically. In fact, many experts believe that the single most important step that can be taken to improve data quality is to establish an effective system of communication between the courts and the repository. In addition, it is important that policies and procedures are established to facilitate the repository's communication with other parts of the criminal justice system in order to improve arrest reporting; create redundancy in the reporting system; and facilitate the updating and correction of records.

Paragraph (k) requires that each criminal history record, or rap sheet, present its information in such a way that a reader can readily recognize arrest, charge and/or disposition entries that are related. At present, rap sheets issued in many jurisdictions fail to link arrest charge and disposition entries. Consequently, it is often impossible to know whether a reported disposition relates to a reported arrest or charge. In addition, paragraph (k) requires that rap sheets bear a legend conspicuously printed on the sheet which contains the date on which the rap sheet was printed and a warning that rap sheet information is current only as of the date of issuance.

Standard 12.2 provides that a state may exempt from compliance information entered into information systems prior to the adoption date of the Standards. This provision is necessary in order to encourage states to implement the most advanced, state-of-the-art data quality procedures for new data. Were state and local criminal justice agencies required to apply Standard 12 to archival data, the administrative burden and the cost could be excessive and, thereby, discourage many agencies from adopting Standard 12.

Research, moreover, indicates that when agencies establish a sophisticated data quality program prospectively so as to apply to new data, the level of data quality improves substantially within just a few years. Older criminal history records are requested and disseminated far less frequently than more current records and, when disseminated, tend to be relied upon less than more current records. Accordingly, it is most important that current data be as accurate and complete as possible.

Standard 13. Dissemination of Criminal Justice Information to Noncriminal Justice Requesters

13.1. All criminal justice information in the possession or control of a criminal justice agency shall be disclosed pursuant to court order.

13.2. All criminal justice information in the possession or control of a criminal justice agency, except criminal intelligence and investigative information, should be made available to qualified persons and organizations for research, evaluative and statistical purposes under written agreements reasonably designed to ensure the security and confidentiality of the information and the protection of the privacy interests of individual subjects. Whenever such information is made available, the identification component of criminal justice records should be deleted unless the purpose of the research clearly cannot be accomplished without such identification information.

13.3. Criminal history record information that has been sealed pursuant to Standard 14 cannot be disseminated except as provided in Standards 14 and 2.5(a).

13.4. All criminal history record information and criminal index information in the possession or control of a criminal justice agency shall be made available to federal agencies pursuant to federal statute for background checks for security clearance determinations or assignment to or retention in sensitive national security duties; and

13.5. All criminal history record information in the possession or control of a criminal justice agency, except nonconviction information and criminal index information, shall be made available, upon request, to any person for any purpose, and nonconviction information and criminal index information shall be made available for governmental or private noncriminal justice purposes as authorized by state statute or court order or rule in circumstances involving responsibility for the life or safety of individuals. Nonconviction information and criminal index information may be made available under this standard only pursuant to a written agreement with the requester reasonably designed to ensure that the information is used only for the purpose for which it was disseminated, is not redisseminated, and is maintained in a manner to assure the security of the information and the protection of the privacy interests of record subjects.

Commentary

Standard 13.1 requires a criminal justice agency to disclose any and all criminal justice information in the agency's possession or control pursuant to a court order. The Standard recognizes that there may well be instances in which the interests of justice warrant the release of criminal justice information to agencies or individuals not otherwise entitled to access. A parallel approach has been taken in the federal Privacy Act which permits disclosure of personal information "pursuant to the order of a court of competent jurisdiction."[30]

Courts should exercise this authority only in circumstances where release is necessary for the effective functioning of the criminal justice process or to avoid an injustice. Ordinarily, release under Standard 13.1 should be authorized by a specific court order directed to a particular agency or individual upon showing of particular circumstances justifying release of this specified information. In such cases, the court order should be expressly tailored to respond to the need shown and to provide adequate security and confidentiality protections.

The exercise of this authority should be limited to courts of general jurisdiction or courts having equivalent jurisdiction. The effect should be to preclude the exercise of this authority by justices of the peace, lesser municipal courts, magistrates and similar courts of limited jurisdiction. The proceedings contemplated by Standard 13.1 may, at the court's discretion, permit the record subject to participate. Courts that are faced with third-party requests for criminal justice information may choose to notify the record subject of the pending request and permit the subject to express his interest in the matter. This procedure is consistent with the approach taken in the Financial Privacy Act and other federal and state statutes governing the release of sensitive, personal information.

Standard 13.2 makes all criminal justice information, with the exception of criminal justice intelligence and investigative information, available to bona fide researchers for evaluative and statistical purposes related to criminal justice, provided that the researcher enters into a written agreement reasonably designed to ensure the security and confidentiality of the information and the protection of the privacy interests of record subjects; and further provided that the researcher not redisseminate the information unless the information is redisseminated in a nonpersonally identifiable format, except in cases where the research purpose clearly cannot be accomplished without preserving identifiers. In view of the substantial benefits that can be derived from research activities, use of criminal justice information for such purposes is encouraged. The anonymity, however, of the record subject should be preserved to the maximum extent possible and every other effort should be made to ensure that record subjects' privacy rights are protected.

For this reason, criminal justice agencies should release criminal justice information for research purposes only upon receipt from the researcher of a written agreement that reasonably establishes the credentials of the researcher and the relationship of the research purpose to a criminal justice purpose. Furthermore, no information should be released unless the agreement provides adequate protection for security and privacy interests. Specifically, the agreement should identify the information to which access is permitted; limit use of the information to the specified research purpose and the approved research design; ensure the security and confidentiality of the information; and, of particular importance, include a nondisclosure provision with penalties for a violation. This approach is consistent with the approach taken in the Department of Justice Regulations governing the "confidentiality of identifiable research and statistical information."[31]

Standard 13.3 makes clear that once criminal history record information is sealed, its dissemination is governed by Standards 14 and 2.5(a). Thus, sealed information is treated as a special category of information. This approach is consistent with the approach taken in the Security Clearance Information Act (SCIA), which exempts sealed information from the dissemination provisions in that Act.

Standard 13.4 would make all criminal history record information in the possession or control of a criminal justice agency available to federal agencies pursuant to a federal statute for background checks for security clearance determinations or assignment to or retention in sensitive national security duties. This Standard is consistent with the approach taken in Standard 1.2 and tracks the federal SCIA. Moreover, Standard 13.4 reflects the view that where legitimate national security interests are at stake, appropriate federal agencies should have access to criminal history record information.

Standard 13.4's requirement that a federal statute be in place is important. The SCIA and the Privacy Act provide substantial protections for state and local criminal justice agencies and record subjects. Standard 13.4's au-

---

[30] 5 U.S.C. § 552a(b)(ii).

[31] 28 C.F.R. Part 22.

thorization for federal access for national security purposes is premised on the assumption that the protections currently embodied in these applicable federal statutes will remain in place. These protections include an exemption for sealed data; a requirement that, at least in some circumstances, federal agency requests for criminal history data be accompanied by fingerprints; an indemnification for state and local agencies in certain circumstances to protect against loss and damage arising from the federal government's use of criminal history data obtained under the SCIA; the right to charge fees to federal agencies for complying with their access requests; limitations on federal agency redissemination or use of the criminal history data for non-national security purposes; and a requirement that the record subject approve requests for his criminal history record data.

Standard 13.5 makes all criminal history information, except nonconviction information and criminal index information, available, upon request, to any person for any purpose; and makes nonconviction information and criminal index information available for governmental and private noncriminal justice purposes, as authorized by state statute or court order or rule, in circumstances involving responsibility for the life or safety of individuals.

This Standard applies to all noncriminal justice requests, whether in-state or out-of-state, other than III requests for noncriminal justice purposes. This Standard recognizes a sharp distinction between conviction and open arrest information on the one hand and nonconviction information and criminal index information on the other. Under Standard 13.5, all members of the public are entitled to access, for any purpose, to conviction record information and to records of open arrests where the arrest has occurred within one year or the arrest is older, but an active prosecution of the charge is pending.

Public availability of conviction record information is consistent with the Justice Department's Regulations for state and local criminal history record systems at 28 C.F.R. Part 20 and the FBI's statutory recordkeeping authorization at 28 U.S.C. § 534. Both the Regulations and the FBI's statute recognize that conviction record information should be more readily available than nonconviction information. At the state level, the law in over 30 states establishes different dissemination policies for conviction information than for nonconviction information. Only three states make all criminal history data, regardless of its character, available to noncriminal justice requesters. Only 13 states make no criminal history data, regardless of its character, available to the public. In every other state, the availability of criminal history data turns, at least in part, on the distinction between conviction and nonconviction data.

Admittedly, only eight states give the general public access to conviction record information, and, even in those states, significant restrictions apply. In a couple of those states, for example, requesters must obtain approval from an administrative board before obtaining access to conviction record information. In other states, a waiver must be obtained from the record subject. Standard 13.5, however, does not have the effect of making conviction record information available to the casual and curious requester. Standard 10.1 permits criminal justice information to be made available only on the basis of positive identification by the means of fingerprints. Accordingly, members of the public seeking conviction record information will have to submit the record subject's fingerprints. As a practical matter, this requirement means that record subjects will have notice of such a request and will generally have given their approval in order for the requester to obtain their fingerprints.

Standard 13.5's approach to the public availability of conviction record information reflects the fact that a conviction record is a formal determination of guilt. Open arrest records, while not reflecting an adjudication of guilt, are nonetheless records of a recent event in which the public interest in access is likely to be high, and the issue of guilt remains to be determined. Moreover, to the extent that conviction record information reflects an adjudication, these records are certain to be publicly available in court docket systems, many of which are now indexed.

Standard 13.5's recommendation that conviction record information be publicly available also reflects the view that there is less chance of unfairness to the record subject with respect to the release of conviction record information. Certainly the most serious type of inappropriate or unfair harm arising from release of criminal history data is the tendency of those records to be incomplete because they lack a disposition and are therefore misleading. This problem is not associated with conviction record information, except to the extent that there may be an appellate determination. Furthermore, to the extent that the release of conviction record information to the public involves a risk of unfairness — in that the record may relate to the wrong person, may arise from an improper conviction or may relate to an old and no longer germane conviction — remedies are available for the individual under the sealing provisions of Standard 14.

Standard 13.5 makes nonconviction information [arrests over one year with no charges actively pending; *nolle prosses*; and acquittals and dismissals] and criminal index information available only pursuant to a state

statute or court order or rule and recommends that such statutes or orders permit access only in circumstances where the noncriminal justice governmental or private purpose at issue involves the life or safety of individuals. Three states have adopted statutes that are essentially "open record" statutes and provide for public access to nonconviction information. A 1979 Wisconsin state court decision lifted the remaining restrictions on the application of Wisconsin's open record statute. In 1980, Florida adopted legislation requiring that all criminal history record information compiled by Florida's Division of Criminal Justice Information Systems be made available to any person, upon request, and the payment of a fee. Florida's statute, however, is limited to criminal history record information that relates to in-state offenses. Most recently, in 1985, Oklahoma adopted an open record statute which makes all criminal history record information available for public inspection. A few other states — North Dakota, Oregon and Nebraska — have adopted statutes that are sometimes characterized as open record statutes but which, in fact, place considerable restrictions upon the public availability of criminal history information. These statutes require requesters to submit fingerprints or a state identification number or require that the agency give record subjects notice of an access request. Legislatures, however, in a number of other states have come close to adopting open record statutes, and many observers predict that in the next few years several states will join Wisconsin, Florida and Oklahoma.

Notwithstanding these "open record" developments, statutes in most states continue to limit governmental and private noncriminal justice access to nonconviction information. Statutes in only about half of the states give governmental, non-national security agencies access to nonconviction information, and then only in limited circumstances and with significant restrictions. Moreover, statutes in only about 10 states give private employers access to nonconviction data and then only in very limited circumstances and subject to substantial restrictions. In recent years, however, a few states have adopted statutes which give private organizations which provide child care services limited access to nonconviction data. Apart from states with open record statutes, no state provides the general public with access to nonconviction information.

In establishing a policy for noncriminal justice access to nonconviction information, SEARCH not only looked at existing state law but also looked at available empirical data. Based on this review, SEARCH recognizes that the empirical data suggest that the release of nonconviction information to the public may not have a significant impact, one way or the other, on the rehabilitation of record subjects and their reintegration into society. SEARCH recognizes that there is evidence that private employers, in particular, may not base employment decisions on criminal history records, particularly arrest-only records, and particularly if there is not a long history of violent or serious arrests. Moreover, SEARCH recognizes that the data suggest that even where employers do use arrest information as a bar to or a restriction on employment opportunities, this may not be significant from a rehabilitative standpoint because recidivism statistics suggest that rehabilitation is seldom achieved regardless of an offender's employment prospects.[32] Moreover, SEARCH recognizes that recidivism rates remain high and that these rates correlate to arrest activity. Accordingly, the public continues to have a significant and legitimate interest in an individual's arrest record.[33] With this in mind, SEARCH's approach to the public dissemination of nonconviction information is not based on the view that preserving the confidentiality of these records will promote rehabilitation or minimize recidivism.

For SEARCH, the motivating consideration for retention of confidentiality standards for nonconviction information is the substantial potential that such records have for causing inappropriate or unfair damage to record subjects in the event that they are released to the public. There are many circumstances in which release of nonconviction information to the public may cast the record subject in a false or inaccurate light and thereby cause inappropriate harm to the record subject. These circumstances can include: 1) where the record relates to a different person; 2) where the record is inaccurate or incomplete; 3) where the record is accurate and complete but it relates to an arrest which is unconstitutional or otherwise improper; and 4) where the record is accurate and complete but it is old and no longer reflective of the individual's character. Admittedly, some of these concerns could be remedied through the sealing provisions in Standard 14. The fact remains, however, that nonconviction information carries an implication of wrongdoing, when, in fact, the record subject may not have broken the law or otherwise engaged in any wrongdoing whatsoever. For this reason, any public release of nonconviction information inevitably runs a significant risk of causing inappropriate harm to the record subject.

Standard 13.5 treats criminal index information in the

32 See note 13, pp. 41-43 and 57-59.

33 Ibid., pp. 60-62.

same manner as nonconviction information. Criminal index information is information indicating that an individual has a criminal history record in a particular jurisdiction (Standard 2.1(c)). Of course, criminal history record data can be comprised exclusively of nonconviction data. Accordingly, release of criminal index information can cause precisely the same harms as release of nonconviction data.

Standard 13.5 permits access to nonconviction information and criminal index information for governmental and private noncriminal justice purposes in circumstances involving responsibility for a life or safety, and where authorized by state statute or court order or rule.

This Standard contemplates that some governmental licensing determinations, and some governmental and private employment determinations, should properly be viewed by the state legislatures and the courts as involving responsibilities for life or safety. For instance, situations in which an individual will be working in or near a residence without supervision; situations in which an individual is charged with ensuring the security or safety of an organization; situations in which an individual will be working with a vulnerable population, such as children or the elderly; situations in which an individual will be authorized to carry a firearm; and situations in which an individual will be authorized to practice in a profession or a trade involving substantial responsibility for life or safety, such as medicine, are all examples of circumstances where Standard 13.5 would accommodate a policy of providing access to nonconviction information.

Standard 13.5 also contemplates that private noncriminal justice access requests can be granted in situations where the individual will be performing appropriate duties on a voluntary basis. Recently, a number of states have amended their laws to expressly authorize noncriminal justice access to nonconviction information in situations such as those referenced above. For example, in the period since 1984, approximately 13 states have amended their laws to broaden access to criminal history information (although not always nonconviction information) to include certain child care providers and to include volunteer organizations that provide services to children, such as the Boy Scouts and the YMCA.[34]

Standard 13.5 limits noncriminal justice access to nonconviction and criminal index information in two additional respects. First, noncriminal justice requesters proceeding under Standard 13.5 must also comply with Standard 10.1, requiring that information be made available only on the basis of positive identification by means of fingerprints. As noted earlier, this requirement effectively means that the record subject will, in most circumstances, have notice of the request and will have authorized the request.

Second, nonconviction information and criminal index information can be made available to noncriminal justice requesters only pursuant to a written agreement that provides that the information will be used only for the purpose for which it was obtained; will not be redisseminated; and will be maintained in a manner to assure security and privacy. These requirements are comparable to the requirements imposed on researchers under Standard 13.2. Moreover, these requirements are comparable to provisions customarily included in user agreements. Many criminal justice agencies currently require that noncriminal justice requesters execute user agreements before they will provide such requesters with criminal history data.

Imposing limitations on noncriminal justice requesters' use and redissemination of nonconviction information is necessary in order for the safeguards in Standard 13.5 to be meaningful. Obviously, if noncriminal justice requesters were free to use nonconviction information for any purpose or to redisseminate the data to any party, then the practical effect of Standard 13.5 would be to make nonconviction data available without restriction. Similarly, reasonable security protections are necessary in order for noncriminal justice requesters to comply with confidentiality restrictions. Finally, the requirement that noncriminal justice requesters who obtain nonconviction information assure that the privacy interests of record subjects are protected means that some reasonable provision must be made for implementing data quality, subject access and the other privacy protections provided for in the Standards.

Standard 14. Sealing and Purging of Criminal History Record Information

14.1. Upon request by a record subject to a central state repository, the central state repository may seal nonconviction information if the record subject can establish to the satisfaction of the repository that, as of the time of the filing of the sealing application, the record subject had not been arrested or charged or convicted in connection with any criminal offense for a period of ten years prior to the date of the sealing application, and provided that, during all of that period, the record subject had been free from confinement or supervision.

---

[34] Ibid., pp. 24-27.

14.2. Upon request by a record subject to a central state repository, the central state repository may seal other criminal history record information if the record subject can establish to the satisfaction of the repository that, as of the time of the filing of the sealing application, the record subject had not been arrested or charged or convicted in connection with any criminal offense for a period of fifteen years prior to the date of the sealing application, and provided that, during all of that period, the record subject had been free from confinement or supervision.

14.3. State legislatures shall exempt from the sealing provisions in Standard 14.1 and 14.2 criminal history record information relating to those types of crimes which, because of their severity or their association with high recidivism rates or because of other factors deemed relevant by the legislature, should not be eligible for sealing.

14.4. A central state repository may unseal criminal history record information sealed pursuant to Standards 14.1 or 14.2 if the central state repository determines to its satisfaction that the record subject has been arrested or charged or convicted after the date on which his records were sealed.

14.5. Upon sealing criminal history record information, a central state repository shall promptly notify other criminal justice agencies within the same state that received the sealed information or contributed such information within the three-year period prior to the sealing. Upon receipt of such a notification, these criminal justice agencies shall promptly destroy or return the sealed information. Upon sealing a record, the central state repository shall also promptly notify all criminal justice agencies outside of the state that have received the sealed information within the three year period prior to the sealing and request that they return or destroy the sealed information.

14.6. Central state repositories shall maintain indexes of sealed records in order to facilitate access to the records for the proper purposes. Access to such an index shall be limited to authorized officials and employees of the central repository who need access for a proper purpose.

14.7. A criminal justice agency may purge criminal history record information whenever the agency deems that the continued existence of the record is no longer useful as a result of such factors as the age of the record subject; death of the record subject; the passage of a substantial period of time without the record subject's contact with the criminal justice system; the nature of the record; the agency's recordkeeping volume or other considerations.

14.8. Any individual who is the subject of a criminal history record may petition an appropriate court at any time to obtain an order to seal the record. The court may issue such an order if it determines that maintenance of the record will cause substantial harm to the record subject and such harm clearly outweighs the criminal justice system's interest in ready availability of the record due to such factors as mistaken arrest, innocence in fact, illegality or unconstitutionality of the underlying statute, rehabilitation of the record subject, or the triviality of the criminal record.

14.9. A court of appropriate jurisdiction may issue an order to unseal criminal history record information whenever the court determines that the benefits of granting access clearly outweigh the record subject's interest in preserving the confidentiality of the data, taking into account such factors as whether the information is needed for sentencing in a subsequent conviction; whether the information is needed to determine eligibility for first offender status; whether a prosecutor or state's attorney has requested the information pursuant to an ongoing investigation or criminal proceeding; and whether the unsealing would protect against a danger to the life or safety of any individual.

14.10. A record subject whose criminal history record information has been sealed may deny the existence of such a record and any arrest or conviction to which it pertains.

Commentary

Beginning with SEARCH's earliest consideration of the privacy issues arising from the retention and dissem-

ination of criminal history records, SEARCH has recommended that these records either be destroyed or sealed when they are too old to have continuing relevance and value or when required by other public policy considerations.

Today, over 35 states have adopted statutes which provide, at least in certain circumstances, for the sealing and purging of criminal history record information.[35] By any standard, however, there is a remarkable amount of disagreement among the states regarding sealing and purging. For example, states disagree about: the definition of sealing and purging; the type of records subject to such orders; the mechanisms for triggering such orders; the substantive criteria for entitlement to such orders; the role of legislative and administrative bodies in setting sealing and purging policies; and the consequences of such orders.

On the other hand, there is not much disagreement about the interests that sealing and/or purging potentially serve. Perhaps the most common, and certainly the least controversial interest, is to exclude from a criminal history record system those records that are no longer useful. The purging provision in Standard 14.7 reflects this interest. For example, records relating to individuals who are older than 70 or 80 are often thought to be of little interest to criminal justice agencies. For this reason, the FBI purges records relating to individuals who are 80 years of age or older.

A second interest often thought to be served by sealing and purging policies is to "reward" and foster the reintegration into society of individuals who have been free of criminal involvement for a substantial number of years. Standards 14.1 and 14.2, and, to a lesser extent, Standard 14.8, reflect this view. This rationale is based, in large measure, on the assumption that individuals who are free of criminal involvement for a substantial period of time are not likely to commit crimes again.

Increasingly, empirical research supports this assumption. Studies indicate that most recidivism occurs within the first three years after release, an arrest or conviction. A Bureau of Justice Statistics (BJS) study, for example, found that "an estimated 60 percent of those who will return to prison within 20 years do so by the end of the third year."[36] BJS also found that "data beyond the three-year mark suggest that some recidivism is likely to occur at least up to five years after release, although at increasingly lower rates."[37]

A third rationale for sealing and purging policies is to exclude records that arguably were never useful. Included in this category are records of mistaken arrests or arrests that were not based on probable cause. Both Standard 14.7 and 14.8 are partly reflective of this interest. It can be argued that these individuals should never have been arrested and, therefore, it makes little sense for criminal justice agencies to maintain a record of such an event.

Some sealing and purging policies are also based on the notion of assuring fairness to a record subject. Standard 14.7 is largely based on this consideration. Records relating to an arrest or to a conviction where the record subject has later "proven" his "innocence in fact" fall into this category. Records that relate to an illegal or unconstitutional arrest or that are based on an illegal or unconstitutional underlying statute also fall into this category.

Another policy consideration that forms a basis for some sealing and purging statutes is the notion that some classes of offenders deserve special consideration. For example, the majority of jurisdictions seal or purge juvenile records, in part, on this basis.[38] As another example, many jurisdictions seal first offender records.

Finally, some jurisdictions seal or purge criminal history records as a response to improper police conduct and a deterrent to such conduct. In these instances, the seal or purge decision is often made without reference to the utility of the record or to concerns for the criminal record subject. Standard 14 does not reflect this policy rationale. Standard 14's overall approach to sealing and purging emphasizes three considerations: (1) that when an individual establishes that the individual has not been

---

35 U.S., Department of Justice, Bureau of Justice Statistics, *Compendium of State Privacy and Security Legislation, 1987 Overview*, NCJ-111097 (Washington, DC: U.S. Government Printing Office, August 1988), pp. 27 and 29.

36 See note 7, *Examining Recidivism*, pp. 1-2; see also J. Markovic, *The Pace of Recidivism in Illinois*, Research Bulletin (Chicago, IL: Illinois Criminal Justice Information Authority, April 1986).

37 U.S., Department of Justice, Bureau of Justice Statistics, *Returning to Prison*, Special Report, NCJ-95700 (Washington, DC: U.S. Government Printing Office, November 1984), p. 2.

38 U.S., Department of Justice, Bureau of Justice Statistics, *Juvenile Records and Recordkeeping Systems*, Criminal Justice Information Policy Series, NCJ-112815 (Washington, DC: U.S. Government Printing Office, November 1988), pp. 24-27.

court may issue such an order if it determines that maintenance of the record will cause substantial harm to the record subject, and such harm clearly outweighs the criminal justice system's interest in the availability of the record due to such factors as a mistaken arrest, innocence in fact, illegality of the underlying statute or other relevant factors.

Courts, not uncommonly, issue orders to seal or purge criminal history record information. In fact, even in the absence of a statutory basis for such orders, courts grant seal or purge requests. Prior to the Supreme Court's decision in *Paul v. Davis* — holding that there is no constitutional protection against the disclosure of arrest record information — many courts based seal or purge orders on constitutional theories.[41] Even in the face of *Paul v. Davis*, some courts continue to find a constitutional basis for the sealing or purging of criminal history record information on the grounds that it is an impermissible impingement on a record subject's right to due process and fair treatment for a criminal justice agency to maintain information about a record subject that is not accurate or complete; that relates to a mistaken arrest; that relates to an arrest made without probable cause; that relates to an arrest or conviction based upon an illegal statute; or that has some other material flaw.[42] In addition, many courts issue sealing and purging orders on the grounds that the courts may use their equitable powers to correct governmental errors and ensure that individuals receive just treatment. Therefore, even in the absence of a statutory basis, courts routinely seal or purge records that are inaccurate, improper, illegal or otherwise defective.[43]

Standard 14.8 is not intended to replace these equitable or constitutional powers. Rather, Standard 14.8 is addressed to state legislatures and urges legislatures to provide statutory authorization for an individual to petition a court for relief where maintenance of a record creates an injustice due to a defect in the record or the underlying event to which the record relates.

Standard 14.9 authorizes a court to unseal criminal history record information when a court determines that the benefits of granting access outweigh the record subject's confidentiality interest, taking into account a variety of factors, including the investigative needs of criminal justice agencies. It is intended that a court could unseal records sealed pursuant to Standards 14.1 and 14.2, as well as records sealed pursuant to 14.8. Thus, Standard 14.9 provides a safety valve in situations where society has a compelling interest in the record which outweighs the interest served by the maintenance of a seal order.

Finally, Standard 14.10 permits a record subject whose criminal history record information has been sealed to deny the existence of such a record and any arrest or conviction to which it pertains. This provision reflects the view that if a record subject can be forced, at his peril, to disclose the existence of a sealed record, the sealing remedy is empty.

Standard 15. Interstate Identification Index

15.1. The Interstate Identification Index (III) should be a decentralized index-pointer system established through adoption by the states and the Congress of an Interstate Compact. The III should be operated by the FBI by means of an automated national index containing only personal identifiers of record subjects whose criminal history records are maintained by central state repositories or by the FBI. The FBI should also maintain a national fingerprint file to provide positive identification with respect to every individual in the III.

15.2. Authority to establish policy for the III, including standards for participation in III, should be vested in the states and such authority should be exercised through an organization, such as the FBI's Advisory Policy Board, with day-to-day system management authority vested in the FBI.

15.3. The primary purpose of III should be to provide information for operational criminal justice use; accordingly, all criminal justice agencies should be authorized direct on-line access to III. Other uses of III, including noncriminal justices uses, should not interfere with the discharge of III's primary mission.

15.4.

(a) In response to a III inquiry for a criminal justice purpose, central state repositories shall provide all criminal history record information, except

---

41 424 U.S. 693 (1976).

42 See SEARCH Group, Inc., *Sealing and Purging of Criminal History Record Information*, Technical Report No. 27 (Sacramento, CA: SEARCH Group, Inc., April 1981), p. 7.

43 Ibid., p. 11

sealed information.

(b) **In response to a III inquiry for a national security purpose, as authorized by federal statute, central state repositories shall provide all criminal history record information, except sealed information.**

(c) **Requests for authorized noncriminal justice purposes shall be made through the central state repository serving the state in which the noncriminal justice requester is located, except for federal noncriminal justice requesters, which may use either the FBI or a repository in a state in which the federal requester is located. In response to a III inquiry for an authorized noncriminal justice purpose, central state repositories shall provide at least conviction and arrest-only entries that are not over a year old or are still actively pending. Repositories receiving records in response to a III request for an authorized noncriminal justice purpose shall release the records to the noncriminal justice requester in accordance with the repository's own state law, which should comply with Standard 13.5. The positive identification requirements in Standard 10.1 shall apply to III inquiries for noncriminal justice purposes.**

Commentary

In 1970, Project SEARCH designed a prototype system for a decentralized index-pointer system for the interstate exchange of criminal record history information. Since that time, SEARCH has steadfastly called for the implementation of a system whereby criminal history records generated by state and local criminal justice agencies would be maintained at the state and local levels rather than the national level. In such a system, records would be located and exchanged through a federally maintained index-pointer. In 1978, the U.S. Department of Justice, through the FBI, began an effort to develop and test the Interstate Identification Index concept.

SEARCH supports the III concept for four reasons: (1) such a system is reflective of and protective of states' rights; (2) such a system is protective of personal privacy; (3) such a system promotes flexibility and effectiveness; and (4) such a system is cost-effective. Standard 15 is reflective of these principles.[44] In particular, Standard 15.1 calls upon the FBI to operate a decentralized index-pointer system containing personal identifiers of record subjects. The legal basis for the III should be established in an Interstate Compact adopted by all 50 state legislatures and the U.S. Congress. Such compacts are customarily used when several states undertake a joint venture such as the III.

The index-pointer system will also identify the state or states (or the FBI) maintaining criminal history record information about the record subject. Central state repositories submit only one entry per individual, even when the individual has multiple entries at the state level, inasmuch as one entry is sufficient to support the "index-pointer" to the appropriate state. Accordingly, the FBI should not maintain duplicate entries from the same state. Standard 15.1 also requires that each index entry in the III be supported by a fingerprint record maintained by the FBI. When the FBI receives notice that a record has been sealed or purged, the FBI should return the fingerprint card to the contributing state.

Standard 15.2 reflects the view that the III is primarily a decentralized, state system. Although the FBI operates the III, the FBI otherwise functions essentially as any state would — contributing index entries for federal offenders and maintaining a federal offender database. During the testing and transition phrases of the III, however, the FBI also functions as a surrogate for those states that do not as yet participate in the III, as well as providing records as needed for states that only partly participate in III. Because the III ultimately is a state system, Standard 15.2 provides that the states should have policy control over the III, including the authority to set participation policies. At present, the states' policy role is exercised through the FBI's Advisory Policy Board (APB).

Unfortunately, the APB's present role is only advisory. Were the APB given authority to establish policy,

---

44 For a more detailed statement of SEARCH's position with respect to the III, see the following policy statements, all of which continue to be effective and none of which is superseded by this Standard: "A Framework for Constructing an Improved National Criminal History System" (April 1978); "Essential Elements and Action for Implementing a Nationwide Criminal History Program" (February 1979); "Implementing the Interstate Identification Index: Issues and Recommendations" (May 1984); and, in particular, *Proposed National Policy for Utilizing the Interstate Identification Index for Access to Criminal History Records for Noncriminal Justice Purposes* (Sacramento, CA: SEARCH Group, Inc., May 1986).

arrested, charged or convicted for a substantial period of time, there is a likelihood that this individual has been rehabilitated, and it therefore makes sense for society to take a "chance" on this individual and seal his records; (2) that there are circumstances in which an individual can demonstrate to a court that the individual's interest in making his criminal history record information confidential outweighs society's interest in the availability of this information due to such factors as a mistaken arrest, innocence in fact, the illegality of the arrest or other factors; and (3) that under some circumstances, a criminal justice agency may determine that a criminal history record is no longer useful and may accordingly decide to purge the record.

As defined in Standard 2.5(a), a record that is sealed is inaccessible except in five circumstances: (1) for record management purposes (including auditing); (2) criminal justice and governmental employment purposes; (3) review by the record subject; (4) research and statistical purposes; and (5) pursuant to statute or court order.

Standard 14.1 provides that, upon request by a record subject to a central state repository, the repository may seal nonconviction information if the record subject can establish to the repository's satisfaction that, at the time of making the sealing application, the record subject had not been arrested, charged or convicted for a period of 10 years, and provided that, during that 10-year period, the record subject had been free from confinement or supervision. Thus, Standard 14.1 provides for an administrative sealing based upon the age of the record. As such, it reflects the view that "old" nonconviction information is unlikely to be reflective of the record subject's character because individuals who recidivate customarily do so within a brief time after release from incarceration or their last contact with the criminal justice system.

Although selection of a 10-year time period inevitably is arbitrary, recidivism research indicates, as noted earlier, that those offenders who are going to engage in criminal conduct are extremely likely to do so within a few years after release. Thus, there is good reason to believe that if an individual has, in fact, been free of contact with the criminal justice system for 10 years, this individual has been rehabilitated. At that point, there is little utility to the criminal justice system in maintaining the individual's record. Moreover, maintenance of the record may do inappropriate harm to the record subject since the record may no longer reflect the record subject's conduct or character. In recognition of these interests, statutes in at least seven states recognize that offenders with old criminal history records present a slight risk of recidivism and, accordingly, these statutes permit the information to be sealed or purged.[39] In addition, a number of courts have ordered the purging of a record after the passage of a substantial period of time. In *Natwig v. Webster*, for instance, a federal district court ordered the purging of a 15-year-old arrest record on the grounds, in part, that the plaintiff had been free of involvement with the criminal justice system since the arrest and the record was no longer reflective of his character.[40]

Standard 14.1 applies to central state repositories rather than to all criminal justice agencies. One reason for this restriction is that only the central state repository is likely to be in a position to make a knowledgeable judgment about whether a record subject has truly been free of contact with the criminal justice system for 10 years. Since central repositories have primary responsibility for maintaining criminal history data, central repositories should take the lead in making sealing decisions. Moreover, even an agency which originally created a record should not seal the record if the record continues to exist at the central repository because, in doing so, the central repository is left without an auditable basis for the record. In view of the key role played by central repositories and the importance of a sealing decision, most of the sealing requirements apply only to central state repositories.

Standard 14.2 applies the same sealing formula to conviction information that Standard 14.1 applies to nonconviction information. The standards differ, however, in that the period of time that must elapse before a record subject can apply to a repository for a sealing order of a conviction is 15 years following final release from confinement or supervision. This distinction is simply reflective of the view — expressed in many of the standards throughout *Technical Report No. 13* — that conviction record information should be far more widely available than nonconviction information.

Standard 14.3 authorizes state legislatures to exempt from the sealing provisions in Standard 14.1 and 14.2 criminal history record information relating to those types of crimes which, because of their severity or their

---

39 The seven states with sealing/purging statutes and the time period after which records are sealed or purged are: Alaska (10 years); Kansas (five years); Massachusetts (10 years); Minnesota (10 years); Nevada (15 years for a felony and five years for a misdemeanor); New Jersey (five years); and Oregon (three years for certain types of offenses).

40 562 F. Supp. 225, 231 (D.R.I. 1983).

association with high recidivism rates or other factors, should not be eligible for an administrative sealing order. These records, however, would still be eligible for a judicial sealing order obtained under Standard 14.8. This Standard recognizes a widely-held view that certain crimes — murder, for example — are so heinous that society should maintain a reasonably available record of those crimes as long as the offender is alive. This standard also recognizes that recidivism patterns for some types of crimes — sex crimes, for example — are quite high, and, therefore, there may never be a time when it is appropriate to seal such records.

Standard 14.3's dependence upon state legislatures to denominate such offenses is a recognition that much research remains to be done concerning recidivism patterns. This dependence is also a recognition that the identification of especially heinous crimes involve normative and controversial issues. Accordingly, it is appropriate for state legislatures to make specific judgments reflective of the norms in their state.

Standard 14.4 permits a central state repository to unseal a criminal history record sealed pursuant to Standards 14.1 or 14.2 if the central repository determines to its satisfaction that the record subject has been arrested, charged or convicted after the date on which the record subject's records were sealed. The basis for an administrative seal under Standards 14.1 and 14.2 is the presumption that the record subject has been rehabilitated and that his record is therefore no longer reflective of his character or conduct. If a record subject is arrested, charged or convicted after obtaining an administrative sealing order, the presumption of rehabilitation is destroyed and there is, therefore, no longer a basis to seal his prior criminal history record information. A number of state sealing statutes permit a sealed record to be reopened upon a subsequent arrest, prosecution or conviction.

Standard 14.5 requires that, upon sealing a criminal history record, a central repository promptly notify other criminal justice agencies within the same state that received the sealed information or contributed the information within a three-year period prior to the sealing. Upon receipt of this notification, these criminal justice agencies are required to destroy or return the sealed information. Standard 14.5 also requires that, upon sealing a record, the central repository will notify all criminal justice agencies outside of the state that have received the sealed information within the three-year period prior to the sealing, and request that they return or destroy the sealed information.

Out-of-state agencies that contributed criminal history record information are not mentioned on the theory that central repositories will not initiate a seal or purge of information that was generated by another jurisdiction. Standard 14.5 requires agencies that receive a sealing notice to return or destroy their in-state copies of the records. These agencies are not permitted to seal their copies because, by definition, sealing permits only employees of the agency maintaining the records to have access to the record for record management purposes only. Consequently, return or removal of a sealed record is necessary in order to ensure that a sealed order, in fact, cuts off disclosure.

The three-year limitation is included because most repositories maintain a log describing each dissemination of criminal history record information for a period of only three years. Accordingly, repositories often will not be able to identify agencies that received the sealed information prior to the three-year time period.

Standard 14.6 requires central state repositories to maintain indexes of sealed records in order to facilitate access to the records for proper purposes. This Standard provides a method for facilitating the unsealing of information. Access to this index, however, should be strictly limited to criminal justice personnel who require access for an authorized purpose. Note that access to this index information is not available through III inquiries.

Standard 14.7 authorizes a criminal justice agency to purge criminal history record information whenever the agency, in its sole discretion, deems that the continued existence of the record is no longer useful. This Standard recommends that agencies take into account the following kinds of factors in setting purge policies: the death of the record subject; passage of a substantial period of time without the record subject's contact with the criminal justice system; the nature of the record; and the agency's recordkeeping volume. This Standard recognizes that criminal history record information should be destroyed when the criminal justice system no longer has an interest in or need for such records. On the other hand, purging is a dispositive remedy and once information is purged, it is gone forever. Accordingly, any formula used to determine the point at which the criminal justice system ceases to have a significant interest in maintaining a record is somewhat arbitrary and is likely to cause controversy. Accordingly, the Standards urge each agency to make its own determination based upon its own needs. It is assumed that criminal justice agencies will act in the best interests of society and will, therefore, not destroy records in which there is any reasonable possibility of continued societal interest.

Standard 14.8 permits an individual who is the subject of a criminal history record to petition an appropriate court, at any time, to obtain a sealing order. The

appropriate, they should be reflected in policy decisions and not as a *de facto* matter in fee policies.

This Standard is consistent with the fee policy in SCIA. With respect to state and local agency charges to SCIA agencies, the SCIA states: "Fees, if any, ... shall not exceed the reasonable cost of providing such information, nor shall they, in any event, exceed those charges to State or local agencies, other than criminal justice agencies, for such information."[47] Note, however, that this Standard is not intended to apply to the processing of III inquiries for noncriminal justice purposes. Fee policies for processing III inquiries (and fingerprint cards) for noncriminal justice purposes are set forth in other SEARCH documents and in APB documents.

Standard 18. Audits

18.1. To the extent practicable, every criminal justice agency maintaining criminal justice record information shall periodically audit their own criminal justice information systems and shall also be subject to periodic audits by an external agency to ensure compliance with these standards.

18.2. Central state repositories shall, at a minimum, conduct annual audits of a representative sample of state and local criminal justice agencies, contributing to or receiving records from the repository chosen on a random basis, to ensure adherence to these Standards. To that end, criminal justice agencies shall maintain appropriate records to facilitate such audits. Such audits shall place particular emphasis on compliance with accuracy and completeness Standards and compliance with the limitations on dissemination.

18.3. Central state repositories' information systems shall also be audited on an annual basis to ensure compliance with these Standards. This audit shall include attention to accuracy and completeness; limits on dissemination; security; and subject access and review.

18.4. State and local criminal justice agencies shall conduct annual audits of their own information systems to ensure compliance with these Standards.

Commentary

This Standard imposes four audit requirements. First, Standard 18.1 requires, as a general proposition, that all criminal justice agencies maintaining criminal justice information be subject to self audits and to independent audits by third parties. More specifically, Standard 18.2 requires state central repositories, at a minimum, to conduct annual audits of a representative sample of state and local criminal justice agencies, chosen on a random basis, to ensure adherence to these Standards. The repository is to ensure that agencies maintain appropriate records to facilitate the audit and that the audit place particular emphasis on compliance with accuracy and completeness Standards and any limits on dissemination. This Standard parallels the requirements in the Justice Department Regulations, 28 C.F.R. § 20.21(e). Standard 18.3 requires that central repositories' criminal justice information systems also be audited on an annual basis. The audit must pay particular attention to accuracy and completeness, limits on dissemination, security, and subject access and review. Finally, Standard 18.4 requires state and local criminal justice agencies to conduct annual audits of their own information systems to ensure compliance with the Standards. Any agency that is assigned or that undertakes an auditing responsibility under this Standard is free to discharge its responsibility by retaining another agency or organization to conduct the audit on behalf of the agency.

Auditing has been demonstrated to be one of the most important elements in the operation of a criminal justice information system. For example, auditing helps system managers and others to determine the degree to which a system is in compliance with applicable laws. Auditing also helps to identify specific problems and, just as importantly, helps to identify particular strategies that can be used to improve system compliance. Furthermore, audits play a role in improving data quality by identifying the extent to which information in the system is not accurate or complete and, in many cases, identifying the causes for such inaccuracies or incompleteness. In addition, audits may create opportunities for improving the relationship between a repository and other state and local criminal justice agencies. Finally, and perhaps most importantly, the process of auditing makes all of the parties participating in the process, both those conducting the audit and those being audited, more thoughtful about the way in which the information sys-

[47] 5 U.S.C. § 9101(b)(1).

tem is being operated and the extent to which information in the system is accurate, complete and timely.

In view of the benefits of auditing, it is not surprising that by the mid-1980s about 30 states had adopted legislation requiring a central repository to audit either state and local record systems, its own system, or both.[48]

Audit methods are not prescribed in the Standards. In keeping with the approach throughout the Standards, the means to implement the Standards are left to each agency to determine in light of that agency's needs, problems and resources. Further, it is recognized that the auditing process can consume resources that are often needed for other important information functions; thus, agencies must have flexibility in designing cost-effective, practicable audit formats.

By way of guidance, Standard 18 contemplates that audits usually will look at the following matters: adherence to the Standards and to applicable law; completeness and accuracy; dissemination procedures; security; and subject access and review procedures.

The methodology for conducting this kind of audit may vary from agency to agency. As a general matter, the Standards contemplate that audits will include an inspection of facilities and equipment; the testing of equipment and procedures; observation of recordkeeping personnel; interviews with management and staff personnel; examination of files, documents and other material; analysis of record samples; and the review of all relevant written Standards, guidelines, regulations, manuals and training materials. It is also contemplated that the audit will include a written report setting forth the audit's methodology and a summary of findings and recommendations. In that regard, agencies are referred to SEARCH's *Audit Manual for Criminal History Record Systems*[49] and *Audit Documentation Guide: A Model Study Approach.*[50]

Standard 19. Sanctions and Penalties

State legislation adopted in conformance with these Standards shall contain administrative sanctions, civil remedies and criminal penalties, including:

(a) administrative action against agencies and officials in the case of serious and repeated violations of the Standards;

(b) private rights of action by persons aggrieved by violations of the Standards to obtain injunctive relief and actual and punitive damages in appropriate cases; and

(c) criminal penalties for willful and knowing violations of the Standards.

Commentary

To ensure the enforceability of the requirements and restrictions in the Standards, state statutes adopted in conformance with the Standards should contain appropriate sanctions, remedies and penalties. The administrative sanctions called for in paragraph (a) would be subject to the appropriate discretion of state and local authorities and may include fines, injunctions, adverse personnel actions, termination of access rights to information or other sanctions, depending upon the frequency, nature and intent of the violations.

With respect to civil remedies, paragraph (b) calls for legislation which provides for private rights of action by individuals aggrieved by violations of the Standards to obtain injunctive relief and to obtain actual and punitive damages.

Paragraph (c) calls for criminal penalties to be included in the state legislation. The penalties would attach only to willful and knowing violations of the Standards. These penalties could include both fines and terms of imprisonment, at levels severe enough to provide a meaningful deterrent. The penalties should be applicable to criminal justice agencies, as well as to individual officials and employees, and to noncriminal justice individuals and organizations. A good faith lack of knowledge or misunderstanding of a particular provision of law or regulation should constitute a defense against punitive civil damage actions and criminal actions, but not against other civil remedies.

---

[48] See note 4, p. 29.

[49] P. Woodard, R. Belair and L. Hoffman, *Audit Manual for Criminal History Record Systems* (Sacramento, CA: SEARCH Group, Inc., December 1982).

[50] P. Woodard, *Audit Documentation Guide: A Model Study Approach* (Sacramento, CA: SEARCH Group, Inc., January 1984).

as opposed to merely advising on policy, and were its membership expanded so as to represent all interested parties while still guaranteeing state control, SEARCH believes that the APB could and should be the vehicle by which the states exercise policy control over the III.

Standard 15.3 provides that the primary purpose of the III is to support operational criminal justice uses. Accordingly, only criminal justice agencies are eligible for on-line, automated access to the III. Other authorized requesters are expected to make requests through the FBI or central state repositories.

Standard 15.4(a) simply reflects the view, set forth in more detail in Standard 7, that criminal justice agencies should be entitled to receive all available III records — all criminal history record information that is automated. It is important to recognize that the dissemination standards in Standard 15 apply only to criminal history data obtained via the III; that is, only automated criminal history data maintained by the FBI or participating central state repositories. Manual records and non-III automated records (generally, criminal history record data pertaining to misdemeanor offenses) are not covered, nor are records maintained by local agencies.

Standard 15.4(b) provides that, in response to a III inquiry for national security purposes, as authorized by a federal statute (presently the Security Clearance Information Act), central state repositories should provide all criminal history record information except, of course, for sealed records. This recommendation is subject to the caveats regarding national security access expressed in the commentary to Standard 13.4.

Standard 15.4(c) imposes four requirements on III inquiries for noncriminal justice purposes: (1) that noncriminal justice requesters authorized to obtain information through a III inquiry (by virtue of the policy apparatus established in Standard 15.2) make their III inquiries through the central state repository serving the state in which they are located, except for authorized federal noncriminal justice requesters, which can make their requests through the FBI or a state repository in a state in which they are located; (2) that in responding to a III inquiry for a noncriminal justice purpose, central state repositories provide at least all criminal history record information, excepting nonconviction information; (3) that repositories receiving records in response to a III request for noncriminal justice purposes release records to noncriminal justice requesters, in accordance with their own state law (which should comply with Standard 13.5); and (4) that the positive identification requirements in Standard 10.1 continue to apply to III inquiries for noncriminal justice purposes.

Standard 15.4 reflects the view that if the III is to be successful, it must satisfy the legitimate needs of authorized, noncriminal justice requesters. If the III fails to satisfy such needs, then the FBI can be expected to continue to maintain a centralized database of criminal history records obtained from state and local agencies in order that the access needs of SCIA agencies, and other noncriminal justice agencies authorized by federal law to obtain criminal history record information, can be met. Accordingly, Standard 15.4 calls for the release of at least all criminal history record information, excepting nonconviction information, in response to a request for a noncriminal justice purpose. Repositories located in states with laws that provide for greater access for noncriminal justice purposes are, of course, free to release more information in response to a III inquiry for a noncriminal justice purpose. All ultimate release decisions, however, should be made not by the state responding to the request (the donor state), but by the state repository initiating the request (the recipient state).

In this way, Standard 15.4(c) is reflective of the recipient state principle expressed in Standard 1.2. Accordingly, when a repository receives criminal history record information in response to a III request for a noncriminal justice purpose, the repository may release less than the total amount of information provided to the repository, in accordance with the law of the state in which the repository is located. Of course, a state which adopted or retained a law which prohibited the release of conviction information to noncriminal justice requesters would not be in compliance with Standard 13.5, which calls upon every state to adopt laws to make all conviction record information available to noncriminal justice requesters and nonconviction information available in circumstances involving responsibilities for life or safety.

Finally, the positive identification requirements in Standard 10.1 continue to apply to III inquiries for noncriminal justice purposes.

Standard 16. Training

Employees who are responsible for handling criminal justice information shall become familiar with these Standards and criminal justice agencies should implement training programs to that end and to make such employees aware of other record-handling laws, policies, procedures and techniques.

Commentary

This Standard requires that employees who are responsible for handling criminal justice information receive training so that they become familiar with the

Standards and with other record-handling laws, policies, procedures and techniques. As is customary, the Standards do not prescribe the means by which an agency will implement this Standard. Depending upon the information in the system, the size and equipment used in the system, the type of agency in which the system is maintained, the number, experience and prior training of the agency's employees, and other relevant factors, system managers will adopt various training strategies. Acceptable methods of training include: the preparation and dissemination of manuals and other written training materials; on- or off-site lecture courses; various on-the-job training programs; and various types of written and other proficiency testing.

Training is viewed as critical, not only because it conveys important knowledge and expertise, but because it conveys a message to information system employees that the handling of criminal justice information in an appropriate and professional manner is important. As long ago as 1970, SEARCH emphasized that information system responsibilities must be treated as equal in importance to other criminal justice functions.[45]

Standard 17. Fees

Criminal justice agencies may charge fees for searching for, and/or making available, criminal justice information for noncriminal justice purposes, and such fees should raise an amount of revenue which approximates, as nearly as practicable, the direct and indirect costs to the agency of conducting the search and/or making the information available.

Commentary

This Standard states that criminal justice agencies may charge fees for searching for and/or making available criminal justice information for noncriminal justice purposes, but such fees should be limited to an amount which approximates the direct and indirect costs of conducting the search and/or making the information available. Of course, it is expected that such fees will not be so high that they effectively deny access rights to authorized requesters. It is emphasized that the decision about whether to charge fees is left to the discretion of each criminal justice agency. Moreover, the amount of the fee is left to the discretion of each agency, except for a recommendation that the fee approximate the direct and indirect costs incurred by the agency in searching for and making the information available. Thus, the Standard contemplates that an agency could charge for its personnel costs, calculated at an appropriate hourly rate, incurred in searching for requested information and reviewing the information to determine if it should be released. In addition, the Standard contemplates that the cost of photocopying a record or otherwise printing a record could be passed along. Further, the Standard contemplates that an appropriate *pro rata* amount for applicable overhead costs could be assigned to each search.

In recent years, it has become relatively common for criminal justice agencies to charge fees for providing criminal history record information to noncriminal justice agencies. By contrast, criminal justice agencies rarely, if ever, charge other criminal justice agencies for searching for or making available criminal history record information. The prevailing view is that the primary purpose for compiling criminal history information is for criminal justice purposes, and, therefore, criminal justice agencies should not be charged. In addition, it does not appear that criminal justice agencies applying such a charge would, in the long run, obtain a benefit because the agency which paid the fee could be expected in the future to charge fees to the agency which collected the fee.

On the other hand, the significant growth in the number of criminal history information requests made by or for noncriminal justice agencies has led many criminal justice agencies to charge noncriminal justice agencies fees. In some repositories, as much as or more than one-half of the total number of search requests come from noncriminal justice agencies. As a consequence, it can be a matter of necessity that criminal justice agencies charge noncriminal justice agencies fees. SEARCH's surveys indicate that, as of the mid-1980s, central state repositories in approximately 30 states charged fees to noncriminal justice agencies.[46] These fees range from a low of approximately $3.00 per request to a high of approximately $15.00 per request. In some states, the fee is imposed administratively, but in about 20 states there is express legal authority for the repository to charge fees.

This Standard reflects the view that criminal justice agencies should not charge requesters an amount that substantially exceeds the agency's search and other costs. When charges substantially exceed costs, the effect of the fee policy is to discourage noncriminal justice requests. When restrictions upon noncriminal justice access are

[45] See note 27, p. 43.

[46] See note 4, p. 37.

Related Reading Materials

Selected from the SEARCH Group, Inc. Annotated Bibliography, the following publications supplement the information found in Technical Report No. 13. *All publications are available from SEARCH upon request.*

Technical Reports

No. 2 *Security and Privacy Considerations in Criminal History Information Systems.* Project SEARCH, July 1970. Report on a project to demonstrate the needs and desires for security and privacy of information contained in computerized criminal history files. Considerations include: types of data in the files, who receives the data, and purposes for which data will be used.

No. 13 *Standards for Security and Privacy of Criminal Justice Information.* October 1975; Second Edition, January 1978. Updates positions taken by SEARCH on the issue of security and privacy of criminal justice information and shapes them into one comprehensive and orderly statement. Aspects are presented in the form of standards, accompanied by interpretative commentary.

Technical Memoranda

No. 3 *A Model State Act for Criminal Offender Record Information.* Project SEARCH, May 1971. Report served as a basis for a Model State Act, which would enhance the efficiency of criminal offender recordkeeping, but with the primary purpose of providing security and privacy protection.

No. 4 *Model Administrative Regulations for Criminal Offender Record Information.* Project SEARCH, March 1972. Report designed as a reference and basis for state administrative regulations to enhance the efficiency of recordkeeping; its primary purpose is to provide guidelines for security and privacy protection. (Directly related to Technical Report No. 2 and Technical Memorandum No. 3.)

Criminal Justice Information Policy

Public Access to Criminal History Record Information. BJS Criminal Justice Information Policy Series, U.S. Department of Justice. November 1988. Evaluates the extent of the availability of criminal history record information to the public and other noncriminal justice requesters.

Conference Proceedings and Workshop Reviews

Proceedings of the National Conference on Open Versus Confidential Records. Bureau of Justice Statistics, U.S. Department of Justice. November 1988. Provides background information on the issues involved, the perspectives of the competing interests for both privacy and openness, and examines the implications of expanding public access.

Interstate Identification Index: Reports and Unpublished Papers

A Framework for Constructing an Improved National Criminal History System. April 1978. Presents a framework for a national criminal history program, and establishes criteria for evaluating alternate approaches.

Essential Elements and Actions for Implementing a Nationwide Criminal History Program. February 1979. Discusses principles for initiatives to produce a nationwide criminal history program, and a detailed description of specific elements of a nationwide program.

Implementing the Interstate Identification Index: Issues and Recommendations. May 1984. This paper discusses the implementation of a national criminal history record program and reviews concerns such as policy control, disposition reporting and record quality.

Proposed National Policy for Utilizing the Interstate Identification Index for Access to Criminal History Records for Noncriminal Justice Purposes. Project SEARCH, May 1986. The proposal discusses the issues of access and dissemination, fingerprints, search requests, fees and implementation approach.

A Proposal for Establishing an Interstate Compact to Implement the Interstate Identification Index. July 1988. The proposal details a number of key provisions that should be included in an Interstate Compact to ensure that the III system will function in a manner consistent with the needs and concerns of the participating state repositories and state and local criminal justice agencies throughout the country.