95782

MF-1

U.S. Department of Justice
Bureau of Justice Statistics

Criminal Justice Information Policy

Intelligence and Investigative Records

95782

U.S. DEPARTMENT OF JUSTICE
BUREAU OF JUSTICE STATISTICS

DR. STEVEN R. SCHLESINGER
DIRECTOR

CAROL G. KAPLAN, DIRECTOR
FEDERAL STATISTICS AND
INFORMATION POLICY DIVISION

PREPARED BY
SEARCH GROUP, INC.

GARY D. McALVEY
CHAIRMAN

GARY R. COOPER
EXECUTIVE DIRECTOR

Report of work performed under BJS Grant No. 82-BJ-CX-0010 awarded to SEARCH Group, Inc., 925 Secret River Drive, Sacramento, California 95831. Contents of this document do not necessarily reflect the views or policies of the Bureau of Justice Statistics or the U.S. Department of Justice.

U.S. Department of Justice
Bureau of Justice Statistics

Criminal Justice
Information
Policy

Intelligence and Investigative Records

NCJ-95787
February 1985

For sale by the Superintendent of Documents, U.S. Government Printing Office

Report Prepared by
Robert R. Belair, Attorney
Kirkpatrick, Lockhart, Hill, Christopher and Phillips
Washington, D.C.

TABLE OF CONTENTS

INTRODUCTION AND EXECUTIVE SUMMARY

This is a report about the collection, maintenance, use and dissemination of personal information in criminal investigative and intelligence files.[1] Because investigative operations are a routine part of police work, and, by contrast intelligence operations are less routine and more controversial, intelligence operations have received far more attention from the media, legislators and the courts. This report gives primary, but by no means exclusive attention to intelligence record information. The report describes the history of investigative and intelligence operations; identifies the legal standards affecting the collection, maintenance and dissemination of this data; and analyzes the policy issues relevant to the handling of this data. Thus, the report is intended to be a comprehensive reference work which compiles and summarizes the literature about intelligence and investigative data.

History

By the turn of this century most municipal police agencies, and virtually all state police agencies, had developed investigative capabilities. By contrast, by the turn of the century, few, if any, criminal justice agencies had as yet developed intelligence capabilities. When criminal justice agencies finally began to develop intelligence operations in the early part of this century, they did so in large measure out of a concern about the threat to domestic tranquillity posed by the influx of aliens and alien political philosophies. The pre-World War I violent anarchist movement, for example, is credited with spurring the emergence of criminal intelligence units within many urban police departments.

Today, many federal and state criminal justice agencies as well as larger metropolitan police agencies, operate criminal intelligence information systems. In

addition, new systems are emerging to promote the sharing of criminal intelligence data among criminal justice agencies.

Collection and Maintenance

Intelligence and investigative information customarily includes data about a broad range of record subjects. In addition, investigative and intelligence data usually is composed of various types of personal information from a wide variety of sources. Suspects, witnesses, victims and their families, and personal and business associates may all be record subjects. Personal information can include detailed information about an individual's personal history, criminal history, educational background and financial background--in short, a full personal dossier. The sources for this information include public records; patrol officers and other police agencies; and informants and witnesses.

Most of the restrictions imposed by law on the collection of personal information are aimed at investigative conduct by law enforcement agencies, and are not aimed at the agencies' information or recordkeeping practices. The Fourth Amendment, for instance, seeks to prohibit unreasonable searches and seizures; the Fifth Amendment seeks to prohibit compelled self-incrimination; and a number of statutes seek to restrict wiretapping and eavesdropping and other types of investigative tactics thought to be intrusive. This report is concerned exclusively with information and recordkeeping practices, and accordingly, does not address investigative or field conduct by criminal justice agencies.

Two types of information collection standards are discussed in this report. First, statutory, regulatory and, to a lesser extent, constitutional standards restrict the circumstances under which a particular individual can be made a target of an investigative or intelligence operation. Second, statutory and constitutional standards place restrictions on agency collection of information about a target's exercise of his First Amendment rights of speech and assembly.

Although many jurisdictions impose relatively detailed maintenance standards upon government agencies which handle personal data, these standards seldom apply to intelligence and investigative information. On those relatively rare occasions when such standards do apply, they take one of four forms: (1) data quality standards which require a minimum degree of accuracy, relevancy or completeness; (2) archival standards which include purging and sealing; (3) format standards which may restrict the holding of intelligence and investigative data in automated systems; and (4) security standards requiring safeguards against improper access to record systems.

Dissemination

The bulk of protections applicable to the handling of intelligence and investigative data apply to the dissemination of such data. Historically, intelligence and investigative data have not been available except within the criminal justice community, and sometimes not even within that community.

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 for criminal justice agencies and their officers for disclosure of intelligence and investigative data. Finally, release of these data may violate record subjects' constitutional rights of due process, or perhaps privacy, if the data is inaccurate or incomplete, and if the release results in a tangible harm to the record subject.

In addition to affirmative confidentiality standards, the federal Freedom of Information Act and similar state laws give agencies discretion to deny requests for access to criminal intelligence and investigative data. To qualify for this exemption from federal and state freedom of information statutes, an agency customarily must be able to show that the information is an investigatory record compiled for a law enforcement purpose and release

would: interfere with enforcement proceedings or a fair trial; be an unwarranted invasion of the record subject's privacy; disclose the identity of a confidential source; disclose confidential investigative techniques or methods; or endanger the life or safety of law enforcement personnel.

Most statutes and court decisions, even ostensibly access laws such as the Federal Freedom of Information Act, permit intelligence and investigative data to remain confidential. However, one body of constitutional law establishes a vague, and still emerging, right of access to government-held records under the First Amendment. Recently, a few courts have held that there is a right of access to intelligence and investigative data unless a statute makes the data confidential.

Policy Issues

Intelligence and investigative information share several key characteristics which make this data extremely sensitive and controversial. First, the quality of the data may be inconsistent, in that the data, of necessity, are often collected from unreliable sources. In addition, intelligence and investigative data often contain extremely personal, sensitive information. Even when the information is not sensitive, the record subject's mere connection with an investigative or intelligence file can be extremely derogatory.

Furthermore, the dissemination, and even the mere maintenance, of intelligence and investigative data can have serious adverse effects on record subjects, including a chilling effect on the subject's exercise of his First Amendment rights, increased police surveillance, and more tangible harms such as loss of employment. Dissemination can also compromise important law enforcement interests in ensuring an effective prosecution, or in protecting the identity of confidential sources or investigative techniques and methods.

For all of these reasons, preserving the confidentiality of intelligence and investigative data has long been a priority for both criminal justice officials and privacy advocates. The importance of confidentiality is further increased by the record subject's inability to review his file, and often his inability to test the veracity or appropriateness of the file in court.

On the other hand, the report points out that intelligence and investigative data share some characteristics which minimize the extent to which such files threaten privacy and due process interests: (1) often information from these files is not retrievable by using the individual's name; (2) information from these files is seldom, if ever, used to make a decision affecting an individual's status, rights or benefits; and (3) as an empirical matter, information from these files is seldom disseminated or used outside of the agency which originally collected the data.

The report discusses two developments which may result in relaxing confidentiality standards for intelligence and investigative data. First, the media and other representatives of the public have argued that as a matter of both law and policy intelligence and investigative data should be more open, particularly after an arrest is made or an investigation is closed. These arguments seem to be receiving a receptive hearing, perhaps, in part, because over the last ten years law and policy have converged to make other kinds of criminal justice information, including arrest and conviction record information, more readily available to the public. Second, there are some signs that organizations and information systems which promote the exchange of intelligence and investigative data within the law enforcement community are emerging.

Description of Report

This report is a reference work. Its purpose is to provide a context in which to place policy developments affecting intelligence and investigative systems. The report is divided into five Parts, and within each Part into two or more chapters.

Part One sets the scene for the discussion which follows. Chapter One in Part One includes a discussion of the definition of the terms intelligence and investigative information and identifies common as well as distinguishing characteristics. Chapter Two presents a brief history of intelligence and investigative operations and related recordkeeping from the Colonial period through to the present.

Part Two provides a brief overview of the operational characteristics of intelligence and investigative information systems. Chapter One in this Part identifies the content as well as the sources for intelligence and investigative information. Chapter Two briefly describes the operation of investigative as well as intelligence information systems.

Parts Three and Four present the legal standards that affect the collection, maintenance and dissemination of intelligence and investigative information. In particular, Part Three identifies the legal standards that govern the collection and maintenance of this information. Part Four identifies the legal standards governing the dissemination of intelligence and investigative information, including a detailed discussion of state and federal freedom of information statutes.

Part Five discusses the policy issues raised by the collection, maintenance and dissemination of intelligence and investigative data.

Finally, the appendices contain a chart describing the characteristics of each state's freedom of information or public records statute and contain a complete table of citations for material used in the report.

PART ONE

THE CONCEPT AND HISTORY OF INTELLIGENCE AND INVESTIGATIVE OPERATIONS AND INFORMATION SYSTEMS

Chapter One

THE CONCEPT OF INTELLIGENCE AND INVESTIGATIVE INFORMATION

Definition of Terms

The terms "investigative information" and "intelligence information" are often used interchangeably. In fact, the two terms describe types of information which are closely related, but which are by no means identical. In this report the term investigative information is defined to mean, "information on identifiable individuals compiled in the course of an investigation of specific criminal acts."[2] Intelligence information is defined to mean, "information on identifiable individuals compiled in an effort to anticipate, prevent or monitor possible criminal activity."[3] Because this report centers on information policy and privacy concerns, it is appropriate to use these definitions, because they define intelligence and investigative information to include personally identifiable information. By contrast, in much of the literature about the intelligence and investigative process, intelligence and investigative data are defined either descriptively so that the definition catalogues information pertinent to solving or anticipating a crime, such as modus operandi information;[4] or defined theoretically so that the definition describes a particular type of analysis as resulting in intelligence information.[5]

Common Characteristics of Intelligence and Investigative Data

The terms intelligence and investigative information, as used in this report, share some common and basic characteristics. First, neither type of information officially documents a formal event in the criminal justice

process such as an arrest, or other formal filing of charges, or a conviction. In other words, intelligence and investigative information can be distinguished sharply from criminal history record information, although intelligence and investigative files often contain criminal history data.

Criminal history record information is usually defined to mean information collected by criminal justice agencies about individuals concerning the individual's arrest or other formal filing of charges against the individual or a conviction or other final disposition along with sentencing, correctional, supervision or release information.[6] In fact, many state criminal justice information statutes expressly define criminal history record information to exclude intelligence and/or investigative information, or they prohibit the commingling of the two types of data.[7]

Second, both intelligence and investigative information, as noted earlier, are comprised of personally identifiable information. Third, as a practical matter, both intelligence and investigative reports are likely to be comprised of similar kinds of personal information--identification data, personal history data, employment and financial information, and information about habits and associations. Fourth, both types of records, as discussed in detail later, are likely to be built on information obtained from the same kinds of sources--public documents, police sources and informants, and witnesses, to name the most important sources.

Distinguishing Characteristics of Intelligence and Investigative Data

While intelligence and investigative data share common characteristics, there is also an important difference between these types of information--the purpose for which the information is created and maintained. Investigative data are compiled for the relatively narrow purpose of identifying the person who committed a particular

crime or otherwise solving the crime. Intelligence information, by contrast, is compiled for the rather broad purpose of identifying a particular individual, or, more often, a group of individuals thought likely to commit crimes in the future.

These differences are illustrated in the language used in Pennsylvania's definition of intelligence and investigative information. Under Pennsylvania law intelligence information is information "concerning the habits, practices, characteristics, possessions, associations, or financial status of any individual." Investigative information is defined as "information assembled as a result of the performance of any inquiry, formal or informal, into a criminal incident or an allegation of criminal wrongdoing, and may include modus operandi information."[8]

Chapter Two

THE HISTORY OF INTELLIGENCE AND INVESTIGATIVE OPERATIONS

A summary of the history of intelligence and investigative activity in the United States is useful in order to put the legal and policy discussions which follow into context.

Early History of Investigative Operations

Investigative activities, if not intelligence activities, have been conducted as a part of routine police work almost from the very inception of organized police activities in this country. Because criminal investigations are such an integral part of any law enforcement agency's mission, the history of investigative operations is a part of and submerged in the history of police activity in this country.

The connection between police activity and criminal investigative work is less pronounced in other societies. In Egypt, Rome and Greece, for example, military units have historically taken responsibility for many criminal investigations.[9] Throughout much of the Middle Ages, crime detection in Western Europe, to the extent that such a thing existed, was largely left to private individuals, often noblemen or other wealthy individuals.[10] Even as late as the 17th century, a crime victim in England who hoped to apprehend his offender would have to purchase investigative services from a minor court official--and even then the chances of obtaining a satisfactory result was slim.[11]

In the United States, the history of criminal investigative activity begins in the mid-19th century. Prior to that time, and beginning in 1636, the nation's cities--even its largest cities--were policed by unpaid and notoriously

undependable night watchmen and a collection of constables and marshals, many of whom were compensated on a per-arrest basis.[12] The colonials had inherited this system from the British.

In Britain too, the night watches were notorious for being comprised of the "dregs of society," and equally notorious for committing as much crime as they deterred.[13] The first full-time crime detective unit was not established in Britain until Magistrate Henry Fielding (author of the novel Tom Jones) created a unit in 1748. It operated out of a court on Bow Street in London and became famous as the "Bow Street Runners." This colorful and much celebrated group was the first to use such basic police techniques as informants, wanted posters and handcuffs.[14]

In 1838, Boston became the first American city to establish a daytime police force. The force was comprised of six full-time officers. In 1844 New York replaced its night watch, which had been in operation since 1656, with a day and night force of several hundred officers. All of these officers had investigative as well as other police duties.[15]

In the Western states, the development of investigative organizations took a different path. Because local police forces were small or non-existent, investigative operations could not develop as an adjunct of local police operations. Instead, by about the middle of the 19th century, several western states established centralized police organizations largely devoted to crime detection. Texas established the Texas Rangers in 1853, and Arizona established its own rangers shortly thereafter. For many of the same reasons, the Canadian Northwest Mounted Police, another famous investigative unit, was established in 1873.[16] By the end of the 19th century, every major urban area, and all regional or state areas, had criminal investigative capacities.

Intelligence Operations in the 19th Century

While the growth of police investigative activity followed more or less naturally from the growth of

general police activity, this was by no means the case for intelligence activity. Indeed, throughout the nation's history the growth and development of intelligence operations has been restricted by two factors.

First, the public, and to a lesser extent, criminal justice officials, have not always perceived a need for intelligence activities. The public, in particular, has always been skeptical that intelligence operations could, in fact, anticipate, prevent or even monitor criminal activity.

Second, the American public has always been ambivalent about criminal intelligence activities because, historically, criminal intelligence has been associated with surveillance of political dissidents.[17] Even former police intelligence officers have expressed ambivalence about the role of domestic intelligence operations and its potential for abuse. One former intelligence official expressed the dilemma as follows. "The challenge to a democratic society is to make intelligence agencies effective representatives of the nation's laws and of the people."[18]

In the 19th century, there was virtually no organized criminal intelligence capability within federal, state or local governments. In fact, during the Civil War, the Pinkerton Detective Agency handled military intelligence for several of the Union Armies.[19] In the decades after the war the "Pinkertons" became infamous by providing intelligence information about labor strife and unionism to industry barons.

Intelligence Operations in the Early 20th Century

It was not until the early decades of this century that professional intelligence units emerged as a part of most large urban police forces.[20] By that time most urban areas were plagued with problems such as loan sharking, fencing, bootlegging, smuggling and narcotics, all of which involved permanent and relatively sophisticated criminal organizations. The emergence of permanent organizations which conducted criminal enterprises

led to a parallel emergence of permanent intelligence organizations to identify and monitor these organizations and, where possible, to anticipate and prevent their criminal activities.[21]

Massive immigration to urban areas in the early 20th century, accompanied by a rising tide of poverty, crime, political extremism and prejudice, also spurred authorities to create special intelligence units. New York City's Bureau of Special Services and Information (BOSSI), for example, was first established in 1912 as the "Radical Bureau." Its primary purpose was to investigate the status of aliens.[22]

The emergence of criminal intelligence units in the early 20th century was also spurred by the violent anarchist movement which had its heyday prior to World War I. Interestingly, early intelligence units were often called "bomb squads." In 1915, New York City changed the name of the Radical Bureau to the "Neutrality Squad" and directed it to "identify bomb throwers, German agents and anarchists."[23]

The Development of Identification Techniques

An important development in the early decades of this century which advanced, and in a real sense made possible, professional investigative and intelligence operations was the development of fingerprinting as a practical, reliable method for obtaining positive identification of suspects and offenders.

The French police were perhaps the earliest to give attention to the problems of positively identifying criminal offenders. As early as 1840 the French began photographing offenders.[24] However, the photographs suffered from poor quality and proved unsatisfactory for use in establishing positive identity.

In the mid-19th century, a French investigator named Alphonse Bertillon developed the Bertillon system, or anthropometry, as it was often called. Bertillon's system measured 11 separate physical characteristics. However, the system was never popular with police officers because of the time and exactitude which its use

required. Its demise in the United States was assured in 1903 when prison authorities at Leavenworth, Kansas used the Bertillon system as part of the processing of a new inmate named Will West. It turned out that the new inmate named Will West had exactly the same Bertillon profile as a current inmate who was also named Will West.[25]

In the early part of this century fingerprinting replaced the Bertillon system as the preferred technique for making positive identification. The "inventor" of fingerprinting, Francis Galton, a cousin of Charles Darwin, estimated that the chances of two individuals having the same fingerprints are one in 64 billion.[26] Today, fingerprinting is the near universal method for obtaining a positive identification.

Intelligence Operations After World War I

World War I and the "Red Scare" immediately following the War helped to further institutionalize police intelligence functions. However, the police role in ferreting out Communist sympathizers also helped to institutionalize the dual mission of intelligence operations--purely criminal investigations and investigations that had a mix of political and criminal characteristics.[27] In 1923, for instance, New York City's intelligence unit received yet another name change. It was renamed the "Radical Squad" and subdivided for the first time into three units, the "Bomb Squad," the "Industrial Squad" and the "Gangster Squad."[28] The "bomb squads'" mission involved primarily surveillance of political radicals.

Prohibition era bootlegging brought massive growth to organized crime and, with it, commensurate growth to criminal intelligence outfits. Federal criminal intelligence agencies saw particular growth during this period. Treasury Department intelligence units were especially active, and their work led to the prosecution of several notorious racketeers, including Al Capone.[29] During that period, in 1924, a small criminal investigative and intelligence unit was also created within the Department of Justice--the FBI.[30]

At the close of the prohibition era, a special rackets group in New York City headed by Thomas E. Dewey produced several celebrated prosecutions, including one which resulted in the conviction of mobster "Lucky" Luciano.[31] At about the same time, the FBI developed the nation's first national intelligence capability and began to promote the systematic exchange of criminal intelligence data among state and local law enforcement agencies and the FBI.[32] In the 1930's, the FBI introduced wiretapping and eavesdropping for intelligence purposes.[33]

The emergence of the FBI as the nation's principal criminal investigative organization had important consequences for criminal justice recordkeeping and information policy. Well before 1900 many law enforcement officials, including most notably Allan Pinkerton, had called for the establishment of a national system to maintain records, and perhaps photographs, of active criminals.[34] As early as 1896 the International Association of Chiefs of Police (IACP) had established in Chicago a file to keep track of active criminals.[35] The FBI took the lead after 1924 in establishing a national repository of information about the identity and criminal history of offenders. At the same time, the FBI took responsibility for disseminating aggregate statistical information about crime, and published its first crime bulletin in 1930.[36] While these activities did not involve the FBI in intelligence information systems, they do reflect a growing awareness at the national level of the critical role played by information and statistics in the criminal justice process.

Intelligence Operations After World War II

In the first two decades after World War II, several developments occurred which encouraged the growth of active and sophisticated criminal intelligence operations. One such development was the growing public perception that the country was threatened by a national organized crime network. In 1950, the United States Attorney

General convened the first national conference on organized crime in response to growing fears about soaring crime rates. Only a few months later, Senator Estes Kefauver began hearings on organized crime that would eventually involve 300 witnesses and make the term "Mafia" part of the nation's vocabulary.[37] In 1954, partly in response to the Kefauver hearings, the Justice Department formed the Organized Crime and Racketeering Section. This represented the Justice Department's first effort, apart from the FBI, to institutionalize a criminal intelligence program.[38]

Just three years later, the newly popularized Mafia received national media attention when over 75 crime syndicate bosses from around the country were photographed converging on Appalachian, New York for what was widely seen as a national convention of crime bosses. Not much later, in 1956, criminal intelligence officers from several states, led by California, formed the Law Enforcement Intelligence Unit (LEIU).[39] LEIU's function is to promote the exchange of criminal intelligence information among agencies represented by member officers.[40]

President Kennedy's assassination in 1963 occasioned a critical review of the intelligence capabilities of the Secret Service, the FBI and the Central Intelligence Agency, as well as many state and local criminal justice agencies. The Warren Commission Report criticized the FBI in particular, and called for expansion of preventive intelligence capabilities.[41]

In 1967 and 1968 two other prestigious commissions issued reports calling upon the nation's law enforcement agencies to improve their intelligence capacities. The Report of the National Advisory Commission on Civil Disorders decried the lack of intelligence information concerning rioting and other civil disturbances:

> Police departments must develop means to obtain adequate intelligence for planning purposes, as well as on-the-scene information

> for use in police operations during a disorder.[42]

In 1967, the President's Commission on Law Enforcement and the Administration of Justice surveyed the status of the nation's criminal intelligence capabilities and found them lacking. Its report called for the "greater exchange of [intelligence] information among federal, state and local agencies."[43] Specifically, the Commission recommended the establishment of regional criminal intelligence information systems, along with the creation of a "central computerized office into which each federal agency would feed all of its organized crime intelligence."[44]

With the establishment in 1968 of the Law Enforcement Assistance Administration (LEAA),[45] substantial monies became available, for the first time, from the federal government for the development of state and local intelligence operations and intelligence information systems. The availability of federal money was important because, historically, police agencies had been reluctant to spend money on the development or operation of intelligence units.[46]

The availability of federal money for intelligence information systems was also important because it encouraged the sharing of intelligence data. In the absence of such encouragement, intelligence officers had shown themselves to be unwilling to share intelligence data, even within their own departments, and certainly not with outside agencies. In consequence, earlier non-federal efforts at establishing regional intelligence systems had failed. For example, a compact among intelligence agencies from the New England states, called the New England Organized Crime Intelligence System, was stillborn in the mid-1960's, despite a promising gestation period.[47]

Intelligence Operations in the 1970's and 1980's

By the end of the 1960's, the criminal justice community was prepared to launch ambitious new efforts to develop intelligence gathering and sharing capabilities. Unfortunately, these ambitious new plans were taking shape just at the moment that thousands of young people were taking to the streets to protest the nation's involvement in the Vietnam War. The result, in retrospect at least, was predictable.

As the volume of political dissidence grew louder, the temptation to use budding intelligence capabilities for surveillance grew apace. By the early 1970's many criminal justice and intelligence agencies were being criticized by the Congress and the media for misusing intelligence capabilities to compile records about domestic political activity.[48] One former intelligence officer for New York City's BOSSI described the situation:

> For [BOSSI], or the 'Red Squad' as some critics called it, the 1950's and early 1960's were the best of times, and the late 1960's and early 1970's were the worst of times.[49]

A series of well-publicized Congressional hearings encouraged the dismantling of many federal domestic intelligence programs and reductions in the funding and size of state and local criminal intelligence programs.[50] During the mid-1970's, with both Watergate and the domestic intelligence scandals fresh in mind, Congress considered several bills that would have substantially restricted the discretion of federal, state and local agencies to conduct intelligence activities.[51] However, none of this legislation was ever enacted.

In fact, by the time the legislation was considered, it may no longer have been needed because of administratively imposed restrictions and budget cutbacks. In 1976, for instance, the Justice Department published regulations which set new, and more restrictive, guidelines for

FBI domestic security investigations.[52] Two years later, LEAA published regulations for state and local intelligence systems funded with LEAA money which placed restrictions on the collection and dissemination of personal data in these systems.[53]

If the 1970's were a decade of scrutiny and retrenchment for intelligence operations, the 1980's may be a decade in which the pendulum swings back toward greater acceptance of intelligence operations. Even as early as 1977, for example, members of Congress decried the erosion in the quality and quantity of federal criminal intelligence data.[54] In 1983 the Justice Department published new, and slightly more relaxed, standards to govern the FBI's domestic security investigations.[55] In 1984, the Senate passed legislation that would strengthen the FBI's ability to maintain the confidentiality of information received from confidential sources, thus presumably encouraging informants to cooperate more fully in the FBI's intelligence investigations.[56]

With this as a brief sketch of the history of investigative and, particularly, intelligence activity in this country, we turn to a description of the operational characteristics of intelligence and investigative data, and a summary of the current status of intelligence and investigative information systems, after which the report will discuss applicable law and policy.

PART TWO

THE OPERATIONAL CHARACTERISTICS AND CURRENT STATUS OF INTELLIGENCE AND INVESTIGATIVE INFORMATION SYSTEMS

Chapter One

OPERATIONAL CHARACTERISTICS

Content of Intelligence and Investigative Information

It is useful to begin with a description of what an investigative or intelligence file looks like. The kinds of personal information contained in intelligence and investigative files tend to be similar. A typical intelligence file will 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.[57] An investigative file about a suspect will contain some, although usually not all, of the same information. Instead, an investigative file will customarily contain more detailed physical descriptions (since the suspect's identity is often unknown, something which is less often the case in intelligence investigations) and less information about background and associates.[58]

Sources for Intelligence and Investigative Information

To obtain personal information, criminal justice investigators look to many sources: witnesses and informants; patrol officers; other criminal justice agencies; photographic or electronic surveillance; physical evidence (often taken from a crime scene); the media and other public sources; neighbors, employers, and associates; and undercover agents.

However, the prime source of information is the least glamorous--public record information. Former Central Intelligence Agency Director Allen Dulles has said, ". . . it is a fact that about eighty percent of all information . . . is obtained openly."[59] Of course, reliance on such prosaic, public sources does not mean that the personal information which they produce is less sensitive. In Tarlton v. Saxbe,[60] for example, the court pointed out that the process of compiling public records "energizes" such records, thereby creating sensitive dossiers.

In a "typical" criminal investigation, investigators take at least some of the following steps to obtain and analyze information: (1) interview the victim, (2) search the crime scene, (3) interview witnesses, (4) record suspect's modus operandi, (5) interview suspects, and (6) prepare files and reports.[61] One police department's investigative manual described this six-step approach as ensuring that information which expertise and study have demonstrated is most likely to solve a crime is "collect[ed] in a structured, organized manner."[62]

Naturally, intelligence investigations are seldom so structured. The form that these investigations take is often determined by whether the agency is conducting what is sometimes called "tactical" intelligence or "strategic" intelligence.[63] Tactical intelligence is aimed at providing information regarding an immediate and specific threat of a criminal event. Consequently, in tactical intelligence operations criminal justice officials customarily collect information which closely resembles the information in investigative files.

By contrast, strategic intelligence, or "pure intelligence" operations aim to produce information about industry-wide or area-wide criminal patterns. Accordingly, strategic intelligence files are likely to contain a wide variety of kinds of personal information about numerous individuals, many of whom may turn out to be innocent of wrongdoing.[64]

Chapter Two

CURRENT STATUS OF INVESTIGATIVE AND INTELLIGENCE OPERATIONS AND INFORMATION SYSTEMS

Today, virtually every law enforcement agency has an investigative capability. Indeed, without an investigative capability the agency would be unable to detect and identify offenders, and thus could scarcely be called a law enforcement agency. However, the size and sophistication of that investigative capacity varies widely. A substantial percentage of agencies, particularly smaller agencies, for instance, does not have plain clothes investigators or a discreet investigative unit. Even in larger agencies, the percentage of sworn personnel assigned to investigative tasks seldom exceeds ten percent.[65]

Far fewer agencies have intelligence capacities, particularly strategic intelligence capacities. Strategic intelligence capacities are typically found in federal and state agencies, large metropolitan police departments and, occasionally, regional task forces or groups. Even in large agencies and departments, the number of sworn officers engaged in intelligence activities seldom exceeds one percent of the force.[66]

Nevertheless, in large agencies intelligence operations are considered indispensable because they operate as the "eyes and ears of the Chief of Police."[67] One former agent for New York City's intelligence unit has expressed this idea as follows:

> Like the Cyclops Polyphemus, the New York City Police Department would be virtually helpless to cope with the many sudden and unexpected public crises without its eyes--the police intelligence unit.[68]

Investigative Operations

In many police agencies, patrol officers have initial and even primary investigatory responsibility for most routine crimes. The investigative policy and procedures manual for a small California city, for example, stresses the investigative role of the patrol officer. "The primary responsibility for the initial investigation of most reported offenses rests with the patrol officer."[69] Similarly, in another California city all criminal investigative duties are assigned to patrol officers.[70] In large police departments, a special investigative unit, or several investigative units, will have responsibility for conducting investigations involving certain types of crimes, such as narcotics or smuggling, or involving certain types of modus operandi.[71]

Investigative Information Systems

Investigative files--unlike intelligence files--are usually organized by a numeric identifier assigned to the crime under investigation. Importantly, investigative files are seldom organized by the name of the investigative subject. It is customary in most agencies to maintain investigative information in a separate filing system apart from criminal history files or the outstanding warrants file (wanted person file).[72] Moreover, investigative files are almost always kept in a manual system under the control of the appropriate investigative unit.[73] The period of time for which the file is maintained is usually a matter of agency discretion, and customarily turns on the prospects for prosecution, the type of crime and the identity and past conduct of the suspect.[74]

The types of personal information and the sources for obtaining personal information found in investigative files have already been described. Typically, this information is recorded in field notes, various reports which in many agencies include a preliminary report (recorded at the time of the first investigation of the crime), progress reports, and a closing and/or prosecution report.[75]

As discussed in detail in subsequent parts of this report, investigative information is ordinarily not released outside of the department which initiated the investigation, except to other law enforcement officials. Even then investigative and intelligence officials are often reluctant to share such data.[76]

Intelligence Operations

Most intelligence texts recommend that the head of an agency's intelligence unit should report directly to the chief of police.[77] However, in practice, intelligence units are often placed within the detective division and the head of the unit reports to the chief of detectives.[78] Many commentators criticize this approach because they fear that it will encourage the intelligence unit to skew information to serve short-term crime detection and criminal apprehension priorities.[79]

The intelligence unit is like no other part of a criminal justice agency-- except, perhaps, an identification division or a criminal history repository--in that the intelligence unit's mission and sole "product" is information.[80] Not surprisingly then, most intelligence agencies devote enormous attention to the collection, compilation, analysis and dissemination of information. According to commentators, successful intelligence units have at least the following three key characteristics.

1. Files containing both biographical and functional information, thoroughly cross-referenced, and arranged for rapid and reliable retrieval.

2. A formal, permanent arrangement for the flow of raw information to the intelligence unit.

3. Persons designated as analysts.[81]

This report has already described the types of personal information customarily collected by intelligence

units and the sources for this personal information. In most intelligence agencies this information is kept in manual files. In addition, almost every intelligence agency has a central log which provides a summary of the content of information received; the date and time of receipt; the source of the information (at least generically); the case number or matter to which the data refer; and the name of the officer to whose attention the information is directed. BOSSI's log was described as follows:

> . . . the daily life of the Bureau evolves around a 24 hour log. The log is comprised of a running account of every significant event affecting the unit . . .[82]

In addition, larger intelligence agencies have several types of specialized personnel to manage and assess this data. An "intelligence interpreter," for example, is used by some agencies to screen new information so that only colorable and potentially relevant data is recorded.[83] As a further example, some agencies use a "criminal source control officer" to manage data obtained from informants or other confidential sources and to manage especially sensitive information.[84]

Intelligence Information Systems

As already noted, intelligence operations are not nearly so common as investigative operations, except to the extent that most large investigative units give some attention to the anticipation and prevention of specific, near term criminal activity. At the federal level, a number of agencies are authorized by statutes to collect personal information for criminal intelligence purposes.[85] At the state level today, virtually every state has established at least one unit within the state police, or within another state agency, which has a criminal intelligence mission.

On a local level, only the largest cities have established permanent intelligence units within their police departments.[86] Some of these local intelligence units operate relatively sophisticated information systems.[87] In addition, a few cooperative ventures among state and local criminal justice agencies or officials operate (or are planning to operate) criminal intelligence information systems.[88]

PART THREE

STANDARDS FOR THE COLLECTION AND MAINTENANCE OF INTELLIGENCE AND INVESTIGATIVE INFORMATION

Chapter One

COLLECTION OF INTELLIGENCE AND INVESTIGATIVE INFORMATION

In most jurisdictions law enforcement agencies have discretion to initiate intelligence and investigative operations, to select the targets of those operations and to determine the types of information about these targets that will be collected. Legislatures, both state and federal, have rarely given the subject detailed attention.[89] Illinois' statute, for example, creates the Illinois Bureau of Investigation and gives it a broad mandate to "investigate the origins, activities, personnel and incidents of crime."[90]

The principal legislative and judicial restrictions placed on intelligence and investigative operations are not aimed at recordkeeping, but rather, are aimed at the methods that agencies use to collect personal information in the course of intelligence and investigative operations. The courts and the legislatures have been far more concerned about police conduct in the field than they have been about imposing information or recordkeeping safeguards.

Much of the reason for that approach is due to the Constitution's concern about safeguarding individuals from abusive police conduct. The Fourth Amendment's guarantees against unreasonable searches and seizures place restrictions on searches of targets' persons, personal effects, houses and papers.[91] The Fifth Amendment guarantees against self-incrimination and limits interrogations and the collection of evidence which depends upon testimonial information or explanations provided by the target.[92]

In addition, numerous statutes, both federal and state, prohibit or restrict certain kinds of governmental information gathering techniques. For example, the Om-

nibus Crime Control and Safe Streets Act of 1968 places restrictions and safeguards on the government's use of wiretapping and eavesdropping.[93] The Privacy Act of 1980 restricts the federal government's use of search warrants to obtain personal information held by the media and certain other recordkeepers.[94] Similarly, the Financial Privacy Act of 1978 establishes a protective scheme to be used by federal agencies attempting to collect financial information about an individual which is held by a financial organization.[95]

This is not to say, of course, that there are no restrictions on the recordkeeping aspects of the collection of intelligence and investigative information. These recordkeeping restrictions fall into two broad categories: (1) restrictions on the circumstances under which individuals can become targets of intelligence or investigative operations; and (2) restrictions on the type of personal information that can be collected about target individuals.

Restrictions on the Targeting of Particular Individuals

Those restrictions which concern when a person can become a target of an investigation are aimed primarily at assuring that an agency has at least some reasonable basis for believing that an individual has been involved in a crime, or is about to be involved in a crime, before the individual becomes a target of an investigation.

LEAA has published guidelines applicable to several federally funded regional intelligence information systems. These guidelines have subsequently been amended and republished by the Office of Justice Assistance, Research and Statistics ("OJARS Guidelines"). They provide that intelligence systems which have received Department of Justice funding can collect and maintain personal information about a particular individual only if it is "reasonably suspected" that the target individual is involved in criminal activity.[96]

The new "Guidelines for FBI Domestic Security Investigations" also contains a standard for targeting individuals. That standard states that domestic security

intelligence investigations can be conducted only when the "facts or circumstances reasonably indicate that two or more persons are engaged in an enterprise for the purpose of furthering political or social goals wholly or in part through activities that involve force or violence and a violation of the criminal laws of the United States."[97]

The City of Seattle adopted an ordinance in 1979 which remains one of the more comprehensive municipal intelligence charters.[98] The Seattle ordinance provides that in order to collect information about an individual in the course of a criminal intelligence investigation, the Seattle Police Department must first have a "reasonable suspicion" that the subject of the information is involved in a criminal activity, or is a victim or witness, and the information sought must be relevant to the investigation. Several states have adopted statutory provisions that are similar to Seattle's formulation. Indiana, for example, prohibits the collection of information about an individual for intelligence or investigative purposes unless "grounds exist connecting the individual with known or suspected criminal activity and if the information is relevant to that activity."[99]

In the mid-1970's, as noted earlier, Congress gave serious consideration to comprehensive legislation, "The Criminal Justice Information Control and Protection of Privacy Act of 1975," S. 2008, that would have regulated the collection, maintenance, use and dissemination of criminal justice information, including criminal justice intelligence information.[100] S. 2008 provided that intelligence information about an individual may be maintained (and such maintenance standards have a de facto effect upon collection) by an agency, "only if grounds exist connecting such individual with known or suspected criminal activity and if the information is pertinent to such criminal activity."[101] Many criminal justice officials opposed this standard because it would have prohibited the maintenance of information about relatives and personal and business associates of target individuals.[102]

During the same period, New York City's Council considered adopting legislation that might have sharply

restricted the collection of personal information for intelligence purposes. The bill provided that any city agency which maintained personal information, for purposes other than the investigation of a specific crime, would have to notify the record subject of the existence of the file and extend the subject other due process rights. New York City intelligence officers argued that many intelligence investigations would be subject to these notice and due process requirements because the investigations would not relate to a specific crime.[103]

In addition to standards that require criminal justice agencies to demonstrate reasonable grounds for connecting a proposed target to a threatened criminal event, many intelligence systems operate under charters which limit their jurisdiction to targets who are suspected of engaging in certain specified kinds of crimes, or who commit crimes involving certain specified industries.[104]

One additional type of standard often affects agency thinking about who should become a target of an intelligence investigation. Federal and some state criminal justice agencies operate under freedom of information statutes which will not permit them to deny requestors access to intelligence information unless the agency can demonstrate that the requested information is "investigatory records compiled for law enforcement purposes."[105]

Thus, in collecting information about a target, most agencies want to be confident that the target's activities are sufficiently related to a criminal activity to permit the agency to claim that the information it collects about the target can be considered "investigatory records compiled for law enforcement purposes." Otherwise the agency will not be able to protect the data from access requests by the public.

For the most part, the courts have been sympathetic to agency efforts to meet this freedom of information act standard. They have held that any "colorable claim" by an agency that an individual may have been, or is planning to be, involved in a criminal activity meets the law enforcement, investigatory records threshold.[106] Nevertheless, the FOIA's investigatory records threshold probably works to establish a de facto collection standard.

Restrictions on the Content of Personal Information

A second type of collection standard regulates the content of information collected in intelligence investigations. Perhaps the most important of these "content" restrictions places limits on the collection of information about an individual's exercise of his First Amendment rights--namely religious, political and civic activities.

The Federal Privacy Act, for example, forbids federal agencies from maintaining any record "describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained, or unless pertinent to and within the scope of an authorized law enforcement activity."[107] Federal law enforcement agencies lobbied hard for inclusion of an exception for law enforcement activities because it permits agencies to conduct investigative operations, if not intelligence operations, much as they did prior to adoption of the Privacy Act.[108]

Indeed, the Privacy Act's legislative history draws a sharp distinction between the activities of "normal dissidents exercising First Amendment rights" and the "activities of individuals or organizations dedicated to the violent overthrow of the government." The activities of the latter are not intended to be sheltered by the Privacy Act's restriction on the collection of First Amendment Information.[109]

To date, there are no published court decisions prohibiting federal law enforcement agencies from maintaining First Amendment information because such maintenance would violate the Privacy Act.[110] However, other types of agencies have run afoul of this prohibition,[111] and its existence quite possibly has an inhibiting effect upon the collection of First Amendment data in intelligence investigations.

To date, over a dozen states have adopted statutes based on the Federal Privacy Act, and several of those state Privacy Act statutes include Privacy Act-type prohibitions on the collection of First Amendment information by state agencies.[112] Moreover, other states have

grafted First Amendment collection restrictions onto their criminal justice information statutes. Indiana, for example, prohibits the collection and maintenance of political, religious, or social information about any individual unless this information is directly related to past or threatened criminal activities and there are reasonable grounds to suspect that the target is or may be involved in criminal activities.[113]

The Chilling Effect Doctrine

The "chilling effect" doctrine propounded by many scholars and accepted by a few courts in the late 1960's and early 1970's posed a significant challenge to the legality of the government's collection of information about individuals' exercise of their First Amendment rights. In 1969 the New Jersey Superior Court issued what may be its most famous decision. In a case called Anderson v. Sills,[114] several civil rights demonstrators and the NAACP sued the New Jersey Attorney General because he had established a domestic political intelligence system under which state and local police compiled and forwarded to the New Jersey State Police information about civil disturbances, riots, rallies, marches and other kinds of protests or demonstrations. The Superior Court held that the establishment of this information system violated the subjects' First Amendment rights of political expression by chilling the exercise of those rights, even though the plaintiffs had not alleged that the existence of this filing system had done them any particular harm.

The plaintiffs' theory rested on an established doctrine that the government cannot interfere, except in the most limited and exceptional circumstances, with an individual's exercise of his rights of free speech and freedom of association. As early as 1958, the Supreme Court had held in a much-quoted opinion, NAACP v. Alabama, that an Alabama court order requiring the NAACP to disclose its membership list was a violation of the NAACP members' constitutional rights because it

interfered with the members' First Amendment right of assembly.[115] The Court reached this holding even though the state had not taken direct action to restrict the NAACP members' right to associate freely.

Despite the earlier NAACP v. Alabama decision, the Anderson opinion provoked a flurry of comment from scholars, police officials and the civil rights and anti-Vietnam War communities.[116] The lower court's opinion in Anderson represented a significant extension of the chilling effect doctrine, because in earlier decisions, including NAACP, the government had taken some kind of affirmative or punitive action aimed at the affected individuals.[117] In Anderson, the alleged chilling effect was ascribed to the mere collection and maintenance of intelligence information.

The chilling effect doctrine, as enunciated in Anderson, posed a serious threat to the collection and maintenance of First Amendment information and, for that matter, to the collection and maintenance of almost any personal information for criminal intelligence purposes. However, in the spring of 1972, the Supreme Court largely disposed of this threat, by publishing their opinion in Laird v. Tatum.[118] Writing for a divided court, split five justices to four, Chief Justice Warren Burger stated that the mere existence and operation of an intelligence gathering and distribution system by the Army did not give the targets of such a system standing to claim that the exercise of their First Amendment rights had been chilled, provided that the targets could not complain of any specific harm that had befallen them.[119]

In the years since the publication of Laird v. Tatum, the courts have continued to reject claims that the mere collection of information about the exercise of First Amendment rights, absent specific, tangible harm to the targets, gives the targets a constitutionally cognizable claim under the First Amendment.[120] However, as noted earlier, targets of this kind of intelligence operation may sometimes have a statutory remedy.

Chapter Two

MAINTENANCE OF INTELLIGENCE AND INVESTIGATIVE INFORMATION

This report uses the term "maintenance" in a generic way to refer to four types of standards which may apply to the holding of personal data. First, data maintenance standards include rules to ensure a minimum level of data quality. Second, data maintenance standards include sealing and purging and archival rules which determine when and how data can be retained in or removed from a record system. Third, data maintenance standards customarily include rules about the format or media in which data can be kept. And fourth, data maintenance standards customarily include rules about system security.

In many jurisdictions, criminal intelligence and investigative systems are not covered by data maintenance rules. Although data maintenance rules are often found in state statutes which regulate the handling of criminal history record information, these statutes typically exclude intelligence and investigative data. As well, data maintenance rules are often contained in state privacy acts, but typically these acts also contain exemptions for intelligence and investigation information.

Data Quality Standards

Perhaps the principal reason that data quality standards are seldom imposed on intelligence and investigative information systems is that, almost by definition, such systems must compile and maintain raw, unverified data. Therefore, if data quality safeguards are applied they usually attach only at the point when the data will be disseminated, and safeguards do not apply when data are merely being collected and maintained.

Notwithstanding the need for flexibility in the maintenance of data in intelligence systems, it is possible to review or audit periodically the content of such systems. The OJARS regulations, for instance, require covered agencies to adopt procedures to "provide for the periodic review of data and the destruction of any information that is misleading, obsolete or otherwise unreliable."[121]

In addition, criminal intelligence experts often exhort intelligence agencies to judge all information for "relevancy and accuracy;" to attempt to verify information from several sources; and to purge information which does not meet minimum standards for relevancy, accuracy and reliability.[122]

Sealing, Purging and Archival Standards

Federal and most state agencies may set their own archival standards for investigative and intelligence records.[123] Alaska's agencies are an exception. Alaska's statute provides that "upon termination of an arrest or police investigation in favor of an individual, information collected must be closed . . . and that information must be expunged within one year after closure." (emphasis added).[124]

Indiana's statute does not establish a specific time period for destruction of intelligence or investigative information, but it does require routine audits of such data. The statute requires that the chief officer of a criminal justice agency maintaining intelligence and investigative data regularly review such data to determine whether grounds exist for retaining the information and, if not, the data must be destroyed.[125]

Seattle's criminal intelligence ordinance includes a provision similar to Indiana's. The ordinance does not establish an express archival standard, but it does require that intelligence records be reviewed and audited every 180 days by an outside auditor. The 180-day audit period presumably encourages the purging of out-of-date or inappropriate data.

Although over 40 states have adopted statutory schemes for sealing or purging arrest or conviction record information, those statutes seldom apply to investigative information and almost never apply to intelligence information.[126] This omission may make sense given that the purpose of sealing and purging statutes is to prevent the dissemination of information that is not accurate or that is no longer probative of a subject's character. Since intelligence and investigative information is seldom disseminated and since, by its very nature, it is expected to contain raw and sometimes inaccurate information, the traditional rationale for sealing or purging is inapposite. However, when intelligence or investigative information is to be disseminated, a stronger argument can be made that the data should first be reviewed for possible purging or sealing.

S. 2008 took precisely this approach. It would have established a national policy for purging intelligence and investigative information. S. 2008 provided that intelligence information:

> may be maintained only if grounds exist connecting such individual with known or suspected criminal activity and if the information is pertinent to such activity. Criminal justice intelligence information shall be reviewed at regular intervals, but at a minimum whenever dissemination of such information is requested, to determine whether such grounds continue to exist, and if grounds do not exist such information shall be purged.[127]

S. 2008's standard for the purging of investigative information would have required data to be purged whenever the statute of limitations for the offense for which the data was collected expired.[128]

In the absence of a statutory authorization, the courts are undecided as to whether, and under what circumstances, they have the authority to order this data to be purged. Several courts have subscribed to a view expressed by the Delaware Supreme Court that the retention of identification records and other types of "informal" records which the police believe are of interest "is a field in which the police have broad discretionary powers which will not be disturbed by the courts save under some exceptional circumstances."[129]

Furthermore, in cases in which the subject of an intelligence record alleges an Anderson v. Sills type of "chilling effect," the courts are virtually unanimous in holding that such an alleged chill of First Amendment interests, without further reason, does not provide a basis for a purge order. In Finley v. Hampton,[130] for example, a federal court of appeals panel held that the maintenance of information in the plaintiff's personnel security file, indicating that two of the plaintiff's friends had "homosexual mannerisms," did not upset any cognizable legal interest or right belonging to the plaintiff. Accordingly, the court found that there was not a basis for a purge order.

In Sikoshod v. Stafford.[131] a Missouri state court reached a similar conclusion in upholding a police department's right to maintain photographs and video tapes of peaceful demonstrations. The court held that the mere maintenance of personal information about the exercise of First Amendment freedoms does not violate a target's constitutional rights, and hence is not a basis for a purge order.

Perhaps the closest that the courts have come to finding a basis in the Constitution for the expungement of intelligence information is set out in Paton v. La Prade.[132] In Paton, a 16-year-old high school student became the subject of an FBI intelligence file when she mistakenly wrote to the Socialist Workers Party seeking information for a high school research project. She had intended to write to the Socialist Labor Party. Her inadvertent inquiry triggered an FBI investigation which included interviews with the local chief of police and with the principal and vice principal of the student's high school.

A federal court of appeals panel held that the high school student had standing to challenge the recordkeeping and that maintenance of an intelligence file about her might so harm her legal interests (undefined by the court) that a basis for an expungement order could be established. According to Paton, a court would have to weigh the harm to the student against the benefits to the government, taking into account: (1) the accuracy and adverse nature of the information; (2) the availability and scope of dissemination; (3) the legality of the collection methods; (4) the existence of relevant statutory standards; and (5) the value of the information to the government.[133] Although Paton seems somewhat at odds with the Supreme Court's earlier holding in Laird v. Tatum, the special facts in Paton provide the best explanation for the court's willingness to consider providing the plaintiff with a remedy.

In at least one case, the court has held that investigative type information should be expunged when related arrest record information is expunged. A federal district court in Urban v. Brier,[134] ordered the expungement of the arrest records of 54 members of a motorcycle gang who were subjected to "dragnet" style arrests without probable cause. The court held that the police should not be allowed to retain fingerprints and photographs of the gang members. The legal basis of this order was not articulated by the court, but it appears to rest on a due process rationale. It is important to note that the record subjects were proper targets. Moreover, the agency's maintenance of the investigative data could reasonably be connected with specific and tangible harm to the subjects--future police harrassment in the form of dragnet arrests.

There is one other basis for the establishment of sealing and purging standards that merits discussion. Federal and state freedom of information statutes often work to establish a de facto purge standard. Those statutes make it relatively easy for agencies to withhold intelligence and investigative information so long as an investigation remains open and a future prosecution is at least a possibility.[135] However, once an investigation is closed, and prosecution is no longer a real possibility, an agency's ability to shelter

investigative and intelligence information diminishes.[136] Although in most jurisdictions agencies retain substantial ability to withhold data, nevertheless, agencies face a threat that record subjects or third parties will be able to use freedom of information statutes to obtain access to investigative and intelligence data once an investigation closes. This threat creates an incentive for criminal justice agencies to purge investigative or intelligence data once an investigation closes.

Format for the Maintenance of Intelligence and Investigative Data

A few jurisdictions have established standards which prescribe, or at least affect, the format, or media, in which intelligence and investigative information can be maintained. Iowa's statute, for example, expressly states that, "intelligence data . . . shall not be placed within a computer data storage system."[137] Similarly, Pennsylvania's statute provides that, "intelligence . . . [and] . . . investigative information . . . shall not be collected in the central repository nor in any automated or electronic criminal justice information system."[138]

The OJARS regulations also set format standards for the maintenance of intelligence data. The regulations provide that if Department of Justice grant funds are used to obtain automated equipment for intelligence systems then "direct remote terminal access to data shall not be made available to system users" and "no modifications to system design shall be undertaken without prior [OJARS] approval."[139]

In a very real sense, the prohibitions found in many state statutes forbidding the inclusion of intelligence or investigative data in criminal history record files or systems also work to encourage the retention of investigative and intelligence data in a manual format. The reason for this is that criminal history record data are increasingly automated. Louisiana, for instance, has adopted perhaps the most detailed statutory standard for the linkage of criminal history data and intelligence and investigative data. The

statute states that criminal history files may be linked to intelligence files in such a manner that an inquiry for intelligence data can include criminal history data. However, the statute further provides that, "a criminal history inquiry response shall not include information which indicates that an intelligence file exists."[140]

Athough legal standards, to the extent germane, work to restrict the automation of intelligence and investigative data, commentators tend to take a different view. One text, for example, cautions that "all newly developed police intelligence filing systems should be compatible with data processing."[141]

Security of Intelligence and Investigative Data

Protecting a record system against improper access is an especially critical data maintenance issue. Surprisingly, most state criminal justice information statutes are silent on the subject. The Federal Privacy Act and comparable laws at the state level do require that government data bases containing personal information be maintained with "adequate" security.[142] Exactly what is required in order to meet the standard of "adequate" security is not apparent from the Privacy Act's legislative history and has not as yet been spelled out by the courts. Moreover, criminal justice agencies are free, at least under the federal act, to exempt investigative and intelligence information systems from this requirement.[143]

The OJARS regulations contain a security standard that is more expansive than the Privacy Act's admonishment. The regulations require covered agencies operating intelligence systems to "establish administrative, physical and technical safeguards (including audit trails) to insure against unauthorized access and against intentional or unintentional damage."[144]

PART FOUR

STANDARDS FOR THE DISSEMINATION OF INTELLIGENCE AND INVESTIGATIVE INFORMATION

Dissemination is probably the most important information policy issue involving intelligence and investigative records. In other words, the key questions are who can see intelligence and investigative information, under what circumstances and subject to what conditions. The short answer is that intelligence and investigative information traditionally has not been available outside the criminal justice community, and often has not been available outside the agency that first collects or compiles the information. Indeed, in most agencies, intelligence and investigative information is not even available to personnel who are not working on the case unless they can demonstrate a need for the data.[145]

A number of factors encourage such tight restrictions on the dissemination of intelligence and investigative data. Criminal justice officials, for example, are customarily loath to share investigative and intelligence data while an investigation is still underway or a prosecution is pending for fear of compromising the investigation or prosecution. In the view of many police officials, there is hardly a quicker or surer way to sabotage an investigation or prosecution than to allow information about the investigation, or sometimes even notice of the existence of an investigation, to come to the target's attention.[146]

Even after an investigation is closed and prosecution is either terminated or otherwise not pending, criminal justice officials may remain concerned about the confidential character of the information. Probably their principal concern at that point is that disclosure may reveal the identity of a confidential source or informant. William H. Webster, Director of the FBI, has been outspoken in defense of law enforcement's need to protect the identity of informants.

> The problem [disclosure of investigative information under the Federal Freedom of Information Act] is no where more sensitive and more important to us than in the protection of confidential sources of information, information furnished to us under a pledge of confidentiality. The informant is the single most important tool in law enforcement.[147]

Law enforcement officials also worry that disclosure of intelligence and investigative information outside of the criminal justice community will reveal an agency's investigative techniques and methods, or will endanger the health or safety of a law enforcement officer or some other individual.[148]

Often, law enforcement officials are not alone in seeking to maintain the confidentialiy of intelligence and investigative information. Usually, the target of the investigation is equally concerned about confidentiality. After all, the mere connection of an individual with a police investigation is considered by most people to be an adverse and unflattering association.[149] Moreover, investigative, and especially intelligence files, may contain extremely sensitive and derogatory data. Some of this data may be unverified and some of this data may be untrue.

In addition to concerns about safeguarding their privacy and reputation, investigative subjects also oppose disclosure of intelligence and investigative information because such disclosure, if prominent enough, may prejudice prospective jurors or otherwise create a climate in which it will be difficult for them to receive a fair trial.[150]

Even the media, by position and custom the unflagging champion of complete public access to all personal data held by criminal justice agencies, have been circumspect in treating the issue of public disclosure of intelligence and investigative information. Many media

spokesmen acknowledge that there are at least some circumstances under which law enforcement agencies ought not to release intelligence and investigative information--even to the media.[151]

What all this suggests is that there are strong policy reasons for maintaining the confidentiality of intelligence and investigative information even after an investigation closes and that, when agencies have discretion to withhold such information, they do exactly that. By and large, the formal legal rules governing the disclosure of intelligence and investigative data sustain agencies' tendencies by prohibiting the release, or at least authorizing the withholding, of intelligence and investigative information.

In this part of the report we look at these formal legal rules under three broad categories: (1) legal rules which set affirmative prohibitions on the release of intelligence and investigative data; (2) legal rules governing agency responses to requests for intelligence and investigative data; and (3) legal rules setting affirmative obligations for the disclosure of intelligence and investigative data.

Chapter One

AFFIRMATIVE STATUTORY PROHIBITIONS ON DISCLOSURE

Despite the existence of strong policy reasons for maintaining the confidentiality of investigative and intelligence data, affirmative statutory prohibitions against the disclosure of such data are scarce. Most frequently, states have made exceptions to their public records laws, authorizing the withholding of intelligence or investigative data. In other words, these state statutes (discussed in more detail in Chapter 5) exempt intelligence and investigative data from affirmative disclosure obligations. One jurisdiction, Alaska, has a statute suggesting that investigative and intelligence data should be confidential, but leaving it to state agencies to adopt regulations to that effect.[152]

In a survey of state statutes, we located statutes that expressly and affirmatively prohibit or restrict the disclosure of intelligence or investigative data in eight states: Indiana,[153] Iowa,[154] Louisiana,[155] Maine,[156] Montana,[157] New Jersey,[158] Tennessee,[159] and Wyoming.[160] Seattle's intelligence regulations take the same approach. Most of these jurisdictions prohibit the disclosure of intelligence and/or investigative data except to other criminal justice agencies.

Indiana's law, for example, states that, "[C]riminal intelligence information is hereby declared confidential and may be disseminated only to another criminal justice agency, and only if the agency making the dissemination is satisfied that the need to know and intended uses of information are reasonable and that the confidentiality of the information will be maintained."[161]

Montana's disclosure prohibition is slightly more relaxed than Indiana's. Montana defines both criminal investigative and criminal intelligence information as

confidential and provides that the, "dissemination of confidential criminal justice information is restricted to criminal justice agencies or to those authorized by law to receive it." Moreover, an agency which accepts confidential information under the Montana law "assumes equal responsibility for the security of such information with the originating agency."[162]

Maine's disclosure prohibition is even broader. Maine bars the release of intelligence and investigative information if disclosure may cause any of the harms enumerated in the federal Freedom of Information Act at 5 USC § 552(b)(7). The information may be disseminated, however, to other criminal justice agencies and the record subject with proper authorization.

Tennessee takes a different approach. Tennessee's public records law states that investigative records "shall not be open to inspection by members of the public" except in compliance with a subpoena or court order, although the records may be inspected by the general assembly on a majority vote, by the governor and by members of the executive branch who are investigating the Tennessee Bureau of Investigation. Under Louisiana's public records law (further discussed in Chapter 5) the disclosure of records revealing the name of a confidential source cannot be compelled even in a court of law except on due process or constitutional grounds.

In addition to the eight states that have adopted express statutory restrictions on the release of investigative or intelligence information, another seven states have adopted restrictive statutes addressed to the disclosure of related information. Related information includes "specified classes of criminal justice information" (Alaska[163]); "statements, photographs or fingerprints required by this article" (Arizona[164]); "personal" information (Arkansas[165]); Department of Law Enforcement records except as needed for identification purposes (Illinois[166]); "evaluative" records (Massachusetts[167]); and "confidential and privileged" information (Oklahoma[168]). The State of Washington prohibits its organized crime intelligence unit "from divulging specific information pertaining to activities of organized crime . . . unless . . . authorized or required to do so by operation of state or federal law."[169]

The OJARS intelligence system regulations take an approach like Indiana's, stating that intelligence data may be disclosed only "where there is a need to know/right to know the data in the performance of a law enforcement activity."[170] According to the commentary issued when the regulations were first published in 1978, the "need to know/right to know" formulation requires that there be an investigation underway, and that the officer have a need for the information--in other words, the information must be relevant to that investigation. The OJARS regulations also provide that, if intelligence data are shared with another law enforcement agency, that agency must agree to follow the regulations' procedures regarding "data entry, maintenance, security and dissemination."[171]

S. 2008 contained what would have been perhaps the strictest standard for the dissemination of intelligence information. That bill would have prohibited the dissemination of intelligence information except to federal agencies for security clearance or employment purposes; or to criminal justice agencies which "need" the information to confirm the reliability of information which they already have; or for investigative purposes "if the agency is able to point to specific and articulable facts which, taken together with rational inferences from those facts, warrant the conclusion that the individual has committed or is about to commit a criminal act and that the information is relevant to the act."[172]

Interestingly, S. 2008 used a different and more relaxed standard for the dissemination of investigative information. Under S. 2008, investigative information could be disseminated to "other governmental officers or employees who have a need to know and a right to know such information in connection with their civil or criminal law enforcement responsibilities.[173]

The Attorney General's Guidelines for Domestic Security/Terrorism Investigations authorize the dissemination of intelligence and investigative data in some

circumstances. The Guidelines authorize dissemination of intelligence information "during investigations" to other federal agencies or state and local criminal justice agencies when such information falls within the recipient agencies' investigative responsibility; or when such information may assist in preventing a crime or act of violence; or for federal personnel security purposes; or as required by law, or Presidential Directive or interagency agreement approved by the Attorney General; or as permitted by the federal Freedom of Information Act or Privacy Act.[174] By implication, the Guidelines prohibit the FBI from disseminating intelligence information under circumstances not covered by its dissemination criteria.

Chapter Two

AFFIRMATIVE COMMON LAW PROHIBITIONS ON DISCLOSURE

Disclosures of intelligence and investigative information outside of the criminal justice community--in addition to violating statutory prohibitions--may also violate tort doctrines of invasion of privacy and defamation. When an agency publicly discloses intelligence or investigative information, the tort doctrine of invasion of privacy, theoretically at least, permits the subject of the disclosed intelligence or investigative information to sue the officers or agency responsible for the disclosure on the theory that this disclosure was either a public disclosure of a private fact or that the disclosure placed the subject in a false light with the public.[175]

Similarly, if an agency publicly discloses intelligence or investigative information, or, for that matter, criminal history record information, and the information is untrue and derogatory, the subject can sue the agency and the responsible officials for defamation. Indeed, disclosure of the very fact that an individual is the subject of an intelligence or investigative file may by itself be defamatory.[176]

However, as a practical matter, the difficulties for plaintiffs in making out a case under any of these theories are so serious that they remain just that-- theories. Plaintiffs very rarely recover from agencies or officials for allegedly improper disclosure of personal information from intelligence and investigative files.

In order to recover, a plaintiff must be able to show that there was a publication of the information to third parties--and some courts have required a relatively large audience before they recognize that a publication has occurred.[177] In addition, a plaintiff must be able to establish that the "facts" disclosed were truly private

facts, if the plaintiff is basing his case on the public disclosure of private facts.[178]

Alternatively, if the plaintiff is suing on a defamation theory, the agency or official charged will be able to avoid liability by demonstrating that the disclosed information is true.[179]

However, by far the most difficult obstacle that a plaintiff must overcome before he can recover against an agency or official for disclosure of intelligence or investigative information is the doctrine of privilege. The courts have held that agencies and their officials have at least a qualified privilege (and in some cases an absolute privilege) to disclose intelligence or investigative information provided that the disclosure is made in good faith; provided that the disclosure can be characterized as a discretionary act, rather than a ministerial act; and provided that it is made to a party with a legitimate need for or interest in the data.[180]

For example, the courts have held, without exception, that law enforcement officials enjoy an absolute privilege to disseminate intelligence or investigative information to other law enforcement officials for law enforcement purposes.[181] Even where the disclosure is to government officials who are not criminal justice or law enforcement officials, the courts have had no trouble holding that the disclosure is absolutely privileged, so long as it is done in the course of the discharge of official duties.[182]

Where the dissemination is to the public, rather than to other law enforcement agencies or government agencies, the potential for liability goes up. Nevertheless, the dissemination may still be privileged if it is deemed to be discretionary, and if some colorable argument can be made that the members of the public receiving the information have a legitimate need for, or an interest in, the information. If the defendant is a federal official he is especially likely to escape liability because federal officials enjoy an absolute privilege for discretionary acts within the scope of their employment.[183]

In Heine v. Raus,[184] for example, a federal district court rejected a complaint for slander and held an employee of the CIA to be absolutely privileged to disclose intelligence information about the plaintiff's alleged contacts with the Soviet KGB. The disclosures were made to members of an Estonian emigre group. The court found that the defendant was merely acting within the scope and course of his employment and carrying out instructions from his employer.

This is not to say, however, that federal agencies and their officials always escape liability for public disclosure of intelligence or investigative information. In Black v. United States,[185] a federal district court awarded a plaintiff $903,232 in damages for tortious invasion of his privacy by the FBI. The FBI electronically eavesdropped on the plaintiff and subsequently released a public statement explaining that the plaintiff had been the subject of the eavesdropping because of his "possible affiliation with organized crime."[186]

The court found that this disclosure severely harmed the plaintiff's livelihood and caused him embarrassment and humiliation.[187] The court further found that the FBI's activities were "intentional." Without so much as a mention of the privilege issue (perhaps because of the court's finding that the FBI officials acted intentionally and thus arguably beyond the scope of their employment), the court held for the plaintiff.

Disclosures to other law enforcement agencies or governmental agencies on the one hand and disclosures to the public on the other represent the "extremes." Perhaps the more "typical" and interesting tort cases involve disclosures to particular private individuals who have an arguably legitimate interest in the information. Patterson v. Supreme Court of Arizona involves this kind of situation.[188]

In Patterson, a police officer disclosed intelligence information to a target's employer in an effort to locate the target. The information at issue was the target's alleged involvement, along with her husband, in physical and sexual abuse of their children. The court refused to

find the agency liable for invasion of privacy, and, in support, cited the fact that commentators have suggested that there is "some logical support for according an officer a qualified or conditional privilege which would protect him from liability for statements made that bear on the prosecution or detection of a crime and that are directed at an individual who is, in some concrete manner, connected in some capacity to that crime."[189]

The court also cited five conditions which must be met before a conditional privilege will be recognized for a law enforcement agency's disclosure of intelligence or investigative information: (1) the disclosure must be made in the aid of law enforcement by an officer discharging his duty; (2) the communication must be made in good faith; (3) the officer cannot repeat a rumor which could easily be found to be untrue; (4) the officer must have jurisdiction; and (5) the officer must actively be preventing a wrong to another or to the public.[190]

In cases where a police agency discloses intelligence or investigative data without being able to meet these kinds of criteria, tort liability can result. In Hyde v. City of Columbia,[191] for example, a Missouri state court said that, where police officers disclosed an abduction victim's name and address even though her assailant was still at large, and in doing so violated internal police rules, the city could be liable to the plaintiff for negligent breach of its duty to crime victims to keep their identities confidential.

Despite occasional decisions such as Hyde v. City of Columbia, the tort doctrines of defamation and invasion of privacy, as a practical matter, have little effect on the disclosure of intelligence and investigative information by criminal justice agencies.

Chapter Three

CONSTITUTIONAL PENALTIES FOR DISCLOSURE OF INTELLIGENCE AND INVESTIGATIVE INFORMATION

Constitutional protections safeguarding personal privacy and due process have a modest effect on the disclosure of intelligence and investigative information. There are two relevant constitutional theories.

The first, and by far the more important of the two theories, holds that criminal justice agencies have a duty to use reasonable procedures to ensure that personal information which they disseminate is accurate and complete.[192] Accordingly, if an agency disseminates inaccurate or incomplete intelligence or investigative information, and thereby causes some specific, tangible harm to the record subject, a court may find a violation of the record subject's constitutionally based due process or privacy interests if the agency does not, in fact, have procedures in place to ensure data quality. If the record subject has sued the offending agency for violation of the federal statute at 42 U.S.C. § 1983, which makes it unlawful to deprive a person of his constitutional rights while acting under color of state law--and this is a likely way in which the constitutional issue would be raised--the individual will also have to show that the agency acted maliciously or intentionally or, at the least, with "aggravated negligence."[193]

Because intelligence and investigative information may be comprised of raw, unverified data, agencies run a risk that this information will turn out to be inaccurate or incomplete. Therefore, criminal justice agencies have a legitimate concern about constitutionally based liability when they disclose such data. Nevertheless, perhaps because such data is infrequently disclosed, or perhaps because actions under 42 U.S.C. § 1983 are so difficult to sustain, our research did not identify a single published

decision in which an agency was found to have violated a record subject's constitutional rights because of the disclosure of intelligence or investigative information.

The second constitutional theory that could, theoretically at least, inhibit the disclosure of intelligence and investigative data holds that the disclosure of criminal justice data, other than conviction data, may violate a record subject's constitutional right of privacy. This theory enjoyed brief popularity in the early 1970's[194] but was severely limited by the Supreme Court in 1976.

In that year the Court ruled, in Paul v. Davis,[195] that arrest record information is a record of an official act not within the sphere of private activities customarily protected by constitutional notions of privacy. Thus, the Court rejected the plaintiff's contention that the public posting of accurate--though dated--information about his arrest was a violation of his constitutional rights under 42 U.S.C. § 1983--at least where the plaintiff could not show any specific, tangible harm that had befallen him as a result of the dissemination.

Chapter Four

STANDARDS FOR RESPONSE TO ACCESS REQUESTS UNDER THE FEDERAL FREEDOM OF INFORMATION ACT

The federal Freedom of Information Act (FOIA) makes all federal agency records available, upon request, to any person, unless the records come within one of nine exemptions set out in the Act.[196] One of those nine exemptions covers "investigatory records compiled for law enforcement purposes, but only to the extent that the production of such records would" result in one of the following six harms:

(A) interfere with enforcement proceedings;

(B) deprive a person of a right to a fair trial or an impartial adjudication;

(C) constitute an unwarranted invasion of personal privacy;

(D) disclose the identity of a confidential source and, in the case of a record compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, confidential information furnished only by the confidential source;

(E) disclose investigative techniques and procedures; or

(F) endanger the life or physical safety of law enforcement personnel.[197]

Even if information is covered by one of the FOIA's exemptions, an agency is still free, as a matter of discretion, to disclose the exempt data, unless some other statute or regulation mandates that the information be kept confidential.[198] The federal Privacy Act is such a statute. It requires that personal information which is accessible by personal identifiers be kept confidential, and thus, for most kinds of personal information, the Privacy Act extinguishes an agency's discretionary authority under the FOIA to release data.[199]

Today, every state has a public records statute which requires state agencies, and in some states, local agencies, to disclose written information to requestors. In approximately ten states the state public records act is identical to or modeled closely on the federal FOIA. Moreover, several courts in those states have said that the federal FOIA's case law concerning the investigatory records exemption is instructive for interpreting and applying the state's investigatory records exemption.[200] In the remaining states the public records statute invariably contains an exemption of some kind for law enforcement investigatory records.[201]

Federal and state freedom of information statutes may pose a significant threat to an agency's ability to preserve the confidentiality of intelligence and investigative information. To the extent that agencies cannot demonstrate that intelligence and investigative information is covered by an exemption the agency is required to make the information available to any requestor. And, once the information is disclosed to one FOIA requestor, it is considered to be in the public domain.[202]

The Meaning of the Phrase "Investigatory Records Compiled for Law Enforcement Purposes"

The courts have defined the phrase "investigatory records compiled for law enforcement purposes" broadly to cover any type of information compiled in connection with a legitimate law enforcement investigation. In Ramo v. Department of the Navy,[203] for example, a

federal district court upheld the FBI's use of the investigatory records exemption to protect information which the FBI had obtained about the plaintiff in the course of an investigation of morale and loyalty of Navy personnel. The court said that to invoke this exemption an "agency need not show that the files reflect a specific suspected violation of the law; however, it must show that the investigation was based on some legitimate law enforcement purpose."[204] Literally dozens of other courts have adopted this standard, or an even broader standard, for identifying investigatory records covered by the exemption.[205]

An Attorney General's memorandum published in 1974 to give agencies guidance about the interpretation and application of the investigatory records exemption argued that the investigatory records exemption could be applied extremely broadly. The Memorandum concluded that "investigatory records are those which reflect or result from investigatory efforts."[206]

Recently, courts have taken a sterner view as to what constitutes investigatory records covered by the exemption. One commentator has remarked, "recent developments suggest that many courts will narrow the applicability of (b)(7) by limiting their willingness to accept "investigative" status for agency records."[207] Recent decisions have held that information about an agency's effort to monitor equal opportunity programs,[208] and information recording an agency's review of draft complaints,[209] are not investigators records within the FOIA's meaning.

In Weissman v. Central Intelligence Agency, a federal appeals panel denied the CIA's attempt to invoke the investigatory records exemption because the court found that the CIA lacked authority to conduct security checks for non-existent employment positions.[210] However, Weissman, and other decisions rejecting an agency's investigatory record characterization, remain the exception. Even in cases where the courts conclude that the agency engaged in "marginal" law enforcement activity, many courts remain willing to uphold an agency's application of

the investigatory records exemption.[211] Furthermore, if information is originally compiled for a law enforcement purpose, the Supreme Court has recently reasoned that the exemption remains applicable, even if the information is subsequently reformulated in a memorandum that is not directly related to law enforcement activities.[212]

Interference with Enforcement Proceedings or a Fair Trial

The exemption at Section 552(b)(7)(A) shelters investigatory records to the extent that production of such records would "interfere with enforcement proceedings." The Supreme Court has held that exemption 7(A) is available while an investigation is underway or so long as there is a prospect "of a future enforcement action."[213] Although the FOIA is a disclosure law and courts are admonished to tilt in favor of disclosure, the courts have usually held that exemption 7(A) is available to protect records, even in dormant cases, so long as there is the possibility of prospective law enforcement action.[214]

Some courts, in an effort to give exemption 7(A) a liberal reading, have gone so far as to hold that the very act of investigating constitutes an "enforcement proceeding" for purposes of invoking the FOIA exemption. In Moorefield v. United States Secret Service, for example, the Fifth Circuit held that a secret service investigation is an enforcement proceeding even though "Service investigations are not directed toward trials and hearings."[215]

A liberal interpretation of the phrase "interfere with enforcement proceedings," such as that provided by the Court in Moorefield, is critical to agencies' ability to withhold intelligence information because, while there is often a "possibility" of a future prosecution in intelligence cases, this possibility is just as often vague and speculative.

Once an intelligence or investigative case is closed, or an action is brought against the target and is concluded, an agency's ability to protect intelligence and investigative information is diminished, but that ability is

by no means extinguished.[216] However, once an investigation is closed the Supreme Court has said that there is a presumption, albeit rebuttable, that investigatory records will be available.[217]

Another factor that encourages disclosure of investigatory records, particularly once an investigtion terminates, is that agencies have a duty under the FOIA to segregate exempt from non-exempt material and to disclose the latter.[218] The courts have been slow to impose this requirement when an investigation is open, on the theory that disclosure of any material may give the subject notice and advantage in a prospective law enforcement action.[219] However, once an investigation terminates, courts insist that agencies carefully identify material which remains exempt and disclose all of the rest of the requested material.[220]

Unwarranted Invasion of Privacy

Even after an investigation terminates, several other exemptions remain available to authorize, where applicable, the withholding of investigative and intelligence information. Exemption 7(C) protects against disclosures of investigatory records compiled for law enforcement purposes which would "constitute an unwarranted invasion of personal privacy" is one of the most important.

This wording is almost identical to the wording of FOIA Exemption 6. Exemption 6 permits the withholding of "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of privacy." The Supreme Court has said that exemptions 6 and 7(C) are to be interpreted and applied in the same manner, except that 7(C) "stands in marked contrast" because the word "clearly" as a modifier of "unwarranted invasion of privacy" is absent.[221]

The purpose of both exemptions is to protect individuals from the public disclosure of intimate details about their lives. Courts apply both exemptions by using a balancing test, weighing the privacy interest of the

record subject against the public's interest in disclosure. However, where exemption 7(C) is at issue, rather than exemption 6, greater weight is given to the individual's privacy interest and therefore the agency's burden of justifying the withholding is lighter.[222]

Maximum Secrecy Maintained if Investigation Ends Without Arrest or Indictment

Depending upon the circumstances, agencies may use one of two different approaches in applying the privacy exemption. First, if an investigation of an individual ends without charges being brought, and thus the very fact that the individual was the target of the investigation may be a secret, the courts tend to uphold the use of 7(C) to withhold all of the investigatory record, even the individual's name.[223]

The courts' rationale seems to be that if the investigation did not produce enough inculpatory, credible evidence to even justify the filing of charges, then the individual is likely to be innocent and the linking of his name to the investigation would be unfairly stigmatizing and defamatory.[224]

Similarly, the courts uphold agency decisions to withhold the names of individuals and information about individuals who are not suspected of wrongdoing, but who appear in intelligence and investigative files. Such people may include victims and witnesses, and the friends and associates of targets of intelligence investigations;[225] individuals participating in the Department of Justice's Witness Security Program;[226] and the FBI agents conducting the investigation.[227]

Only Personal Facts Withheld if Existence of Investigation Made Public, or if Target Arrested or Indicted

The second way in which agencies are permitted by the courts to use the privacy exemption is far more restrictive. Courts uphold the use of the exemption to protect from disclosure intimate personal details which

are unrelated to the suspected violation of law (and hence of little public interest), and which are extremely sensitive and personal (and hence result in a demonstrable privacy violation if disclosed). Agency use of the privacy exemption in this kind of selective manner customarily occurs when the individual has already been linked publicly to the investigation, and thus the privacy interest to be preserved is an interest in avoiding disclosure of intimate, non-germane personal data.

> Decided cases clearly indicate that under normal circumstances, intimate family relations, personal health, religious and philosophic beliefs, and matters that would prove personally embarrassing to a person of normal sensibilities should not be disclosed.[228]

The courts have also characterized personal financial information, at least where unrelated to allegedly criminal activities, as private, intimate information deserving of protection.[229]

On the other hand, the courts have consistently held that information about professional and entrepeneurial activities, and information directly related to the conduct that led to the suspected violation of law, is not the type of information intended to be protected by the 7(C) exemption.[230] In Stern v. Small Business Administration, for example, a federal district court rejected an agency's claim of privacy under Exemptions 6 and 7(C), saying that the purpose of the FOIA's privacy exemptions is to protect individuals from public disclosure of intimate details of their personal lives, not to protect against the disclosure of information about professional and business relationships.[231]

Similarly, in Board of Trade of the City of Chicago v. Commodity Futures Trading Commission, the court rejected the use of Exemption 6 to shelter information held by the Commodities Futures Trading Commission

which consisted of identification information and commercial information about individuals in the commodities industry. The court said that the commerical aspect of the data and the absence of any intimate personal details made the individual's privacy interest extremely slight.[232]

Every 7(C) privacy claim must be decided on a case by case basis by balancing the public interest in the intelligence or investigative data against the target's privacy interest. In balancing the target's privacy interest against the extent of the public's interest in disclosure, the courts have said that the interest to be served must be a true public interest (although the requestor's private interests can be served at the same time). Thus, mere idle curiosity or private financial gain will not meet the public interest test, and hence will not outweigh even a very minimal privacy interest.[233]

Furthermore, the courts have found that, after an individual is arrested, the extent and legitimacy of the public's interest in the individual is enhanced, and conversely, the individual's privacy interest is, to some extent at least, forfeited or waived. Thus, once an arrest occurs, the arrest information and related investigative data are less likely to qualify for protection under the FOIA's privacy exemption. In Tennessean Newspaper Inc. v. Levi, for example, a federal district court upheld the disclosure under the FOIA of contemporaneous arrest information, and related investigative data, on the grounds that the arrested individual had waived his privacy interest and the public had a legitimate interest in this data by virtue of the individual's arrest.

According to the Tennessean Newspaper court, disclosing requested information about persons arrested or indicted for federal criminal offenses does not involve substantial privacy concerns. The Court cited several factors to support this conclusion.

> First, individuals who are arrested or indicted become persons in whom the public has a legitimate interest, and the basic facts which identify them and describe generally the investigations and their arrests become matters of legitimate public interest. The lives of these individuals are no longer truly private. Since an individual's right of privacy is essentially a protection relating to his or her private life, this right becomes limited and qualified for arrested or indicted individuals, who are essentially public personages.[234]

Disclosure of the Identity of a Confidential Source or Information Obtained from a Confidential Source

The FOIA's exemption for confidential source data is another confidentiality protection which survives the termination of an investigation or prosecution. Indeed, protecting the identity of a confidential source is one of the primary reasons law enforcement officials seek to keep intelligence and investigative information confidential. Exemption 7(D) of the federal FOIA permits federal agencies to withhold investigatory records compiled for law enforcement purposes to the extent that production would "disclose the identity of a confidential source and, in the case of a record compiled by a criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, confidential information furnished only by a confidential source."

In 1979 FBI Director William Webster brought Congress a list of more than 100 instances in which the FOIA, notwithstanding the availability of the 7(D) exemption, failed to protect adequately the identity of a confidential source. By 1981, Judge Webster's list of such instances had grown to 204 examples.[235]

Numerous members of Congress have indicated that they share Judge Webster's concerns. Senator Orrin

Hatch, for example, has expressed his concern about federal law enforcement agencies' ability to protect the confidentiality of information in intelligence and investigative files supplied by confidential sources:

> To date no fewer than five different reports on the FOIA have uncovered extensive harm to the ability of law enforcement officers to enlist informants and carry out confidential investigations.[236]

Concern about safeguarding informants' identities, among other things, has led Senator Hatch to introduce legislation to amend the FOIA and to broaden the exemption for intelligence and investigative data.[237]

Although law enforcement agencies are dissatisfied with the FOIA's exemption for informant identities and informant-supplied information, the courts have broadly applied the exemption to shield such information. In Dunaway v. Webster,[238] for example, a federal district court reassured law enforcement agencies that the burden to be placed on them to establish the confidential nature of a source or informant is "minimal."[239]

Investigative Techniques, and Life and Safety of Law Enforcement Personnel

The FOIA's exemption at Section 552(b)(7)(E) protects against the disclosure of information about confidential techniques and procedures used in law enforcement investigations. To invoke this exemption successfully, an agency must be able to demonstrate that the information to be produced, if disclosed, would reveal confidential, non-routine techniques and methods.[240]

The FOIA's exemption at Section 552(b)(7)(F) protects against the disclosure of investigatory records compiled for law enforcement purposes which would endanger the physical safety of law enforcement personnel. In order to invoke this exemption successfully, an agency must be able to demonstrate a reasonable likelihood that disclosure of the requested intelligence or investigative information would endanger a law enforcement official.[241] Of course, even if such a showing is made, the exemption usually is applied only to the name and other data that would identify a law enforcement official.

Chapter Five

STATE FREEDOM OF INFORMATION ACTS

Two generalizations can be made about state freedom of information statutes: (1) every state has adopted a freedom of information statute; and (2) in virtually every state, intelligence and active investigative data are exempt from the reach of the disclosure requirements of these statutes by express statutory provision or case law.[242]

State freedom of information statutes fall into three broad categories: statutes containing investigatory records exemptions which are substantially identical, or similar, to the exemption in the federal FOIA; statutes with investigatory records exemptions that are different from the federal standard; and statutes containing no express exemption, leaving the issue to be addressed by other statutes or case law.

Jurisdictions which have adopted freedom of information statutes that take the same approach toward shielding investigatory records as does the federal statute are: Connecticut,[243] the District of Columbia,[244] Louisiana,[245] Maryland,[246] Michigan,[247] and South Carolina.[248] Included in this category are statutes that contain slight variations on the federal exemption scheme. Louisiana strengthens the exemption for confidential source data by mandating that records which would disclose the identity of a confidential source not be disclosed, and that no court may order their disclosure except on grounds of due process or constitutional law.

Two states provide, in statutes other than their public records law, for the nondisclosure of investigative records on grounds similar to those contained in the federal FOIA: Kentucky[249] and Maine.[250] New York's statute permits law enforcement agencies to withhold all records that could cause any of the harms enumerated in

the federal FOIA--not just investigative or intelligence records.[251]

States which have adopted different exemption formulations for investigative or intelligence information include California,[252] Delaware,[253] Massachusetts,[254] Minnesota,[255] Nebraska,[256] Oregon,[257] Pennsylvania,[258] Rhode Island[259] and Vermont.[260]

Several of these states, including California, Nebraska, Oregon and Rhode Island, establish a blanket exemption for intelligence or investigative data, and provide that such data need not be disclosed pursuant to an access request. California's statute states that, with certain exceptions, nothing in the state's freedom of information act "shall be construed to require disclosure of . . . records of complaints or to investigations conducted by, or records of intelligence information or security procedures of, the Office of the Attorney General and the Department of Justice, and any state or local police agency . . ."

Freedom of information statutes in states such as Massachusetts establish a standard for release of investigative and intelligence data which, while falling short of a blanket exemption, nonetheless works to shelter data more readily and fully than does the exemption standard in the federal FOIA. Massachusetts' statute permits police agencies to withhold investigative materials which, if disclosed, could detract from effective law enforcement to such a degree as to operate in derogation of the public interest.[261] Factors which courts consider in establishing a derogation of the public interest include the discouragement of police initiative or candor.[262]

Colorado and Delaware have adopted statutory exemptions for intelligence and investigative information which give criminal justice agencies holding the data relatively broad discretion to weigh the public interest in disclosure against the public interest in confidentiality and to decide accordingly.

Delaware permits agencies to withhold "intelligence files compiled for law enforcement purposes, the disclosure of which could constitute an endangerment to the local, state or national welfare and security."[263]

Under a few state freedom of information statutes, investigative data receive less protection than under the federal FOIA. Minnesota's statute, for instance, provides that active intelligence and investigative information is non-public.[264] However, inactive investigative information is public unless release would jeopardize another ongoing investigation or reveal the identity of an undercover agent, an informant, a crime victim, or a witness who has asked for confidentiality.

As noted above, in some states, investigative and intelligence records are not expressly exempt from disclosure requirements of the freedom of information statute, but an exemption is nonetheless implied by the courts, at least for records of ongoing investigations. Thus, in Arizona, the state attorney general has said investigative reports need not be released to the public upon request. Instead, the information should be carefully scrutinized and withheld if it is confidential or if disclosure would be detrimental to state interests.[265]

Arizona's appeals court took the same approach in Little v. Gilkinson,[266] holding that the test for nondisclosure of investigative material is whether it would have important and harmful effects on the official duties of a law enforcement agency.

In Georgia, a court has held that police may withhold information regarding ongoing investigations, the names of informants and, under exceptional circumstances, the names of complainants.[267] However, in Houston v. Rutledge, Georgia's Supreme Court held that once a criminal investigation is concluded and the file closed, either with or without prosecution[268] by the state, the investigative records, in most instances, should be available for public inspection.[269]

Minnesota and Georgia illustrate that, in some states, investigative and intelligence data are subject to public release more readily under state or court construction than they would be under the federal FOIA. Nonetheless, freedom of information statutes in most states work much as does the federal FOIA to exempt most investigative and intelligence data from compulsory disclosure requirements.

Chapter Six

ACCESS BY RECORD SUBJECTS, INCLUDING LITIGANTS, TO INTELLIGENCE AND INVESTIGATIVE INFORMATION

Subjects of most types of criminal justice information, such as arrest or conviction record information, enjoy special, and nearly complete, rights to review, and often to obtain a copy, of such information.[270] Indeed, today the subjects of many types of personal information have a right to inspect and obtain a copy of their records.[271] However, the subjects of intelligence and investigative data possess no such special access rights.

Access by Record Subjects Who Are Not Litigants

Except in instances in which the government uses intelligence and investigative information to make final decisions affecting an individual's interests, the record subject is not viewed as having special access rights to such data. Moreover, many of the interests served by withholding intelligence and investigative data apply just as appropriately to instances in which the record subject seeks such data as they do to instances in which third parties seek such data.

In particular, agency concerns about avoiding interference with enforcement proceedings and safeguarding information supplied by confidential informants are just as germane--if not more germane--when record subjects seek access to intelligence and investigative data about themselves. The only interest served by withholding intelligence and investigative data that are not at issue, when the record subject seeks the data, is the protection of the record subject's privacy.

Consequently, federal and state statutes do not provide record subjects with access rights to their intelligence and investigative data. Moreover, the courts have

had no trouble seeing a difference between subject access requests for intelligence and investigative data and subject access requests for other types of personal data.

Thus, in Superintendent, Maryland State Police v. Aenschen,[272] a Maryland court denied a record subject access to state police investigatory information about him compiled in connection with the revocation of the record subject's right to carry a handgun. Similarly, in Nunez v. Drug Enforcement Administration,[273] and Marshall v. New York State Police,[274] the courts held that disclosure of investigatory records to a record subject would be improper because it would reveal the identities of confidential sources, as well as confidential techniques and methods.

The federal Privacy Act, and similar laws now effective in over a dozen states, do give record subjects a right of access to federal and state information about them respectively, subject to certain procedural and substantive exceptions.[275] However, one of the substantive exceptions in the federal act, and most of the state acts, permit agencies to exempt intelligence and investigatory material compiled for law enforcement purposes from the subject access requirements.[276]

Access by Litigants

The only significant exception to the rule that record subjects do not have special access rights to intelligence and investigative information applies when the record subject is a defendant or litigant in a proceeding---and provided, of course, that the proceeding was not brought for the express purpose of obtaining access to the intelligence and investigative data.[277]

Most courts have held that when a litigant needs access to his intelligence and investigative information to defend himself in a criminal proceeding, the Fifth Amendment's due process protections and the Sixth Amendment's fair trial protections require the production of relevant intelligence or investigative data.[278]

The courts have also recognized a few other situations in which litigants should be given access to investigative and intelligence data which concerns them. For example, where police misconduct is at issue in a civil suit and the police attempt to withhold relevant intelligence and investigative data from a record subject, the courts have ordered the intelligence and investigative data to be released to the record subject. Moreover, where a government agency harms an individual--by, for example, releasing derogatory information about the individual--the courts have said that the record subject may have a right to discover the basis for the derogatory information, even if that involves access to intelligence and investigative data.[279]

In those instances where courts have denied litigants access to intelligence and investigative information, the information at issue usually relates to other parties;[280] or release of the information will interfere with an enforcement proceeding, or with some other compelling societal interest.[281]

Chapter Seven

AFFIRMATIVE DISCLOSURE REQUIREMENTS

This report has already discussed those statutes which make intelligence and investigative data confidential as a mandatory matter. The report has also discussed those statutes which give law enforcement agencies discretion to withhold intelligence and investigative data. We turn now to a discussion of those sources of law which place affirmative legal obligations upon agencies to disclose intelligence and investigative data.

Although many jurisdictions make certain types of criminal justice data public--police blotter information and conviction record information most often fall into this category--[282] few, if any, states have adopted statutory provisions which require agencies to release intelligence or investigative data. To the extent that there are colorable arguments for mandatory release of intelligence and investigative data, those arguments are based on constitutional, and in particular, First Amendment principles.

The Supreme Court has acknowledged that the First Amendment gives the press and the public at least a limited right to obtain access to government-held documents. Moreover, the Court has upheld the right of the media to publish intelligence and investigative information (usually victim information) once the information is contained in a public record, or is otherwise lawfully obtained by the media.[283] However, at the same time, the courts have resisted specific attempts by the press and the public to use the First Amendment to pry open government closed files.[284] In most instances in which the courts have confronted this question, they have upheld statutory confidentiality provisions in the face of arguments that such provisions are unconstitutional.[285]

CONTINUED

1 OF 2

In Black Panther Party v. Kehoe,[286] for example, a California court upheld the constitutionality of an exemption in the state's public records act which permits agencies to withhold investigatory records. The court said that although there is a connection between First Amendment freedoms and access to government files, the connection has not been defined or substantiated. The court concluded that the California legislature, in authorizing the withholding of investigatory records, had demarcated a limited area of confidentiality which did not run afoul of First Amendment guarantees.[287] The court reasoned that the legislature could balance the competing public interests of disclosure and confidentiality and could opt for the latter.

A couple of cases have gone a little further in articulating a First Amendment right of access to intelligence or investigative information. In Houston Chronicle Publishing Co. v. Houston,[288] the court upheld the constitutionality of Texas' open records act's provision exempting from public disclosure records of law enforcement agencies dealing with the detection and investigation of crime. The court acknowledged, however, that the statute placed a burden on the public's constitutional "right to know." Nevertheless, the court concluded that this interest must be balanced against the state's interest in protecting the integrity of future prosecutions and protecting subjects' privacy interests.

Recently, the Wyoming Supreme Court has also analyzed the extent of the government's obligation under the First Amendment to make government-held documents available to the public. Sheridan Newspapers, Inc. v. City of Sheridan, held that the constitutional right of access may be conditioned by statutory restrictions and balanced with relevant competing interest considerations, and, therefore, a provision in Wyoming's open records law exempting investigatory record information was constitutional.[289]

While there is nothing new about this holding, the Sheridan opinion makes several important points. First, the court goes on record--more expressly and pointedly

perhaps than any prior court--that there is a "constitutional right of access to police records."[290] Second, the court indicates that this right of access can be limited only by legislative fiat. Thus, the court held that a police department could withhold investigative data from a requestor only when acting under statutory authorization. Third, the court's opinion suggests that a court should look at the reasonableness of the legislature's basis for authorizing the withholding, and strike down a statute if it is not based on relevant, competing interest considerations. Finally, the opinion finds that the Constitution establishes a presumption that police records are publicly available, and that legislatures must meet a relatively heavy burden in order to overcome this presumption.

Sheridan is the strongest pro-disclosure opinion yet to be published which concerns access to intelligence and investigative data. It remains to be seen whether Sheridan presages a judicial move toward further acceptance of constitutional arguments in favor of the disclosure of intelligence and investigative data.

PART FIVE

POLICY CONSIDERATIONS CONCERNING THE HANDLING OF INTELLIGENCE AND INVESTIGATIVE DATA

Chapter One

CHARACTERISTICS OF INTELLIGENCE AND INVESTIGATIVE DATA

Policies for handling investigative, and especially intelligence, information have almost always been considered controversial.

Intelligence and investigative data have a number of characteristics which help to explain such controversy. First, personal data collected in intelligence and investigative operations may be raw and unverified. Much of the data consists of second and third-hand reports. Sometimes, of course, this information turns out to be incorrect.

In addition, the subject of an intelligence or investigative file almost never has an opportunity to inspect his file. The record subject's lack of participation in the recordkeeping process makes it more difficult to discover errors in the file. Moreover, the subject's exclusion (as well as third parties' exclusion) makes the whole system less accountable. This secrecy inevitably fosters myths and misconceptions about investigative and intelligence systems.

In addition, because many intelligence or investigative operations never result in prosecutions, the subject may never get his day in court to challenge the accuracy of data. In other words, if inaccurate, incomplete, untimely or irrelevant information, much of which may be extremely sensitive or derogatory, is in an investigative or intelligence file, it may just as likely as not remain in that file.

Another characteristic of intelligence and investigative information that makes this information so controversial is its inherently derogatory nature. The mere association of an individual with an intelligence and investigative operation usually damages the individual's reputation, and as well, may cause the individual signifi-

cant, tangible injury. Studies indicate, for example, that most employers do not distinguish between arrest information and conviction information.[291] Although there are no surveys on the subject, it is possible that employers make little distinction between an individual who has been, or is, the target of an investigative or intelligence operation and an individual who has been arrested. One unreported decision from Oregon, for example, involved an individual who lost his job because of a record of a police investigation and detention.[292]

Moreover, being identified as a subject of an investigative or intelligence file is not simply a matter of namecalling. Rather, as Justice Douglas noted in Joint Anti-Fascist Refugee Committee v. McGrath,[293] it is an official government designation of status, and it is likely to be taken seriously by recipients of this information.

Indeed, even if the information is never disseminated, the subject of an investigative or intelligence file may suffer harm. Some commentators argue that an individual who has been the target of one such investigation--even if the investigation never leads to an arrest--is more likely, simply by virtue of his past status, to be the target of future police activity.[294] Targets of law enforcement investigations may also suffer what commentators and courts have characterized as a "chilling effect" on the exercise of their First Amendment and other constitutional rights.

Of course, it must be pointed out that intelligence and investigative information possess several characteristics which minimize the threat which these kinds of records pose to a record subject's privacy and due process interests.

First, intelligence and investigative information is often not indexed or organized by the name or other identifiers of the target individual. Instead, this information may be organized by the crime under investigation, the business entity or industry under investigation or some fanciful project name. As a consequence, the information is far less likely than name-indexed records such as criminal history record data, to pose a privacy threat to

the target individual once the investigation closes. In recognition of this fact the Privacy Act only applies to records which are accessible by a personal identifier.[295]

Second, intelligence and investigative information is seldom used to make a decision about the status, rights or benefits of an individual. Moreover, if the information is subsequently used as a basis for some adverse action against an individual, such as a grand jury indictment, the individual is likely to have a chance at that time to rebut the evidence on which the indictment, or other action, is based. Thus, intelligence and investigative files are not administrative files (i.e., decisionmaking files). The Privacy Protection Study Commission did not recommend that subject access and other kinds of due process protections be extended to non-administrative files.[296]

Third, there is little evidence that intelligence and investigative information is imporperly disseminated or used. As discussed in detail in this report, criminal justice officials have a strong interest in maintaining the confidentiality of this data. It appears that by and large these officials have faithfully maintained the confidentiality and security of such data. Indeed, criminal justice officials are more often criticized for failing to share relevant investigative and intelligence data with other officials in their agency or in other criminal justie agencies than they are criticized for overbroad dissemination.

Chapter Two

COLLECTION, MAINTENANCE AND DISSEMINATION POLICY

For intelligence and investigative data policymakers have experimented with three types of policy initiatives: collection restrictions, maintenance restrictions and dissemination restrictions. However, collection and maintenance restrictions have enjoyed less popularity than dissemination restrictions.

Collection Issues

There is wide agreement that law enforcement agencies must collect personal data for investigative purposes. Indeed, without an investigative capability, law enforcement agencies would quite simply be unable to perform their primary mission of identifying and apprehending violators. There also seems to be agreement that law enforcement agencies should be able, with restrictions, to collect personal information for intelligence purposes.[297] However, there remains little consensus about two key collection questions: what standards should govern who becomes a target of intelligence and investigative efforts; and should any restrictions be placed on the type of personal information gathered during these investigations?

As to who becomes a target, privacy advocates argue that law enforcement agencies should have a factual basis for believing that an individual is engaged in activities that involve or will involve a violation of the law before they make that individual a target of an investigation. Law enforcement officials tend to argue for a more lenient standard which gives agencies discretion to collect information about an individual whenever statements, circumstances or facts reasonably indicate

that the individual is engaged in activities which involve or will involve a violation of law.[298]

Law enforcement officials point out that investigative, and particularly intelligence operations, must be broadly structured to collect all relevant information, and that the imposition of strict standards for obtaining personal information would scuttle many investigations before relevant facts emerge.[299] As noted earlier, the Attorney General's guidelines for domestic security and terrorism investigations have recently been modified to give the FBI greater discretion in deciding to launch an investigation and in identifying potential targets.[300]

The second collection issue centers on whether restrictions should be placed on the content of personal information collected (or maintained) in intelligence and investigative files. The primary content restriction which has been imposed to date has limited agencies' collection of data concerning an individual's exercise of his First Amendment rights. As discussed earlier, the federal Privacy Act and similar state privacy statutes restrict the collection of First Amendment information--albeit in a manner which leaves most law enforcement agencies free to collect such information for authorized law enforcement purposes.[301]

Generally, law enforcement officials have argued that they should not be hampered by content restrictions imposed by legislators who oftentimes have little idea of how to conduct an investigation. They point out that the very nature of intelligence and investigative operations require agencies to obtain a broad range of personal information, and that there is no way to anticipate what piece of information may be relevant, or to frame general rules for collection that can work in all kinds of investigations.[302]

Many privacy advocates, and certainly most legislators, have accepted these arguments. There seems to be a consensus, however unsteady, that investigative and intelligence operations are necessary, and that law enforcement agencies must be given significant discretion to collect personal information about individuals who they

believe may be engaged in activities which involve, or will involve, violations of law.[303]

Maintenance Issues

In general little effort has been made to impose data quality standards on intelligence and investigative information systems. This result is attributable, no doubt, to a concern that agencies must be free to maintain raw and unverified data.

Furthermore, there has been comparatively little effort to construct archival standards, format standards or security standards for intelligence and investigative information systems. Two factors probably account for lawmakers' seeming reluctance to impose these kinds of recordkeeping standards. First, until recently policymaking for intelligence and investigative operations was left largely to agency discretion. Second, because intelligence and investigative data are seldom disseminated many policymakers believe that they pose, at most, only a modest threat to subject due process and privacy interests.

In recent years, lawmakers have shown a greater propensity to dictate information standards for intelligence and investigative data. Moreover, if intelligence and investigative data become more widely available, pressures may increase for the imposition of data maintenance standards.

Dissemination Issues

Historically, investigative data, and particularly intelligence data, have been available within the agency which originated the data only on a strict need to know basis. Outside of that agency, other criminal justice officials customarily are able to obtain such data only if they can demonstrate that they have a need for the data in an ongoing investigation, and that they will not redisclose or otherwise misuse the data. Investigative and intelligence data have been virtually unavailable to all other kinds of third parties.

In part, this emphasis on confidentiality is a function of custom and usage. And, in part, too, this emphasis on confidentiality flows from the operational characteristics of intelligence and investigative information systems. In this regard, three characteristics are especially important: (1) intelligence and investigative data are often not accessible by name, thus making it hard to tie to a specific individual; (2) intelligence and investigative data are usually segregated from rap sheet data; and (3) these data are usually maintained manually.

In part, too, strict confidentiality accorded intelligence and investigative data results from concern by law enforcement officials that the identities of their confidential sources be kept secret; that prosecution prospects not be impaired; and that special investigative techniques and methods not be compromised. Finally, part of the emphasis on confidentiality stems from the unique capacity of this data to harm unfairly subject individuals if the data are released--in other words a concern about individual privacy.

Despite the traditional confidentiality protections which attach to intelligence and investigative data, three emerging phenomena may change existing standards for data exchange or disclosure. First, some observers believe that there is a policy trend toward opening some types of criminal justice record information, most particularly criminal history record information. In keeping with this trend representatives of the media and of various private sector interests argue that at least some intelligence or investigative data ought to be released once an investigation is closed or an arrest is made.[304] If an investigation is closed, the law enforcement agency's interest in preserving confidentiality, while not eliminated, is reduced. Conversely, if an arrest is made, the individual can be said to have waived some of his right to privacy and, at the same time, the public's interest in the individual increases.[305]

The media and other observers also argue that some degree of access to investigative, and particularly intelligence, files is beneficial for oversight purposes. Oversight may discourage agencies from maintaining inappropriate information or discourage them from using information for improper purposes.[306]

It remains to be seen whether these arguments will influence lawmakers, or whether the combined weight of law enforcement community and privacy advocates will outweigh arguments for opening intelligence and investigative data. The Congress' recent willingness to consider seriously amendments to the federal FOIA that would strengthen agencies' ability to withhold investigative and intelligence data suggests that law enforcement arguments in opposition to openness have been influential.[307]

On the other hand, constitutional case law, if not the FOIA case law, seems to be tilting in the direction of openness. This trend may be significant in light of the judiciary's and the legislatures' movement, over the last ten years, toward opening criminal history data to public inspection.[308]

A second phenomenon which may eventually alter traditional policies tending to discourage the exchange of intelligence data is the emergence of regional intelligence information systems. In the view of many lawmakers and law enforcement officials, the routine and effective exchange of intelligence data among participating criminal justice agencies and officials is a necessary and inevitable response to the growing organization and sophistication of criminal enterprises, particularly those involved in illegal drugs, smuggling and white collar crime.[309]

A third phenomenon which may alter traditional data exchange practices is the rapid spread of automated information technology. The Privacy Protection Study Commission, a two-year federal research effort, concluded that the computer's prodigious archival and retrieval capabilities makes it far easier (and cheaper) to collect, store and disseminate personal information--it's simply easier than ever to say yes to dissemination requests.[310]

Furthermore, today, research data bases, police blotters, court dockets, and other previously manual, nonname indexed sources of public information are becoming

name indexed, automated data bases. What this may mean is that information, once public, will remain readily accessible. Thus, to the extent that investigative and intelligence operations leave public footprints--in the form of newspaper articles or court or station house records, for example--those footprints leave permanent "fossilized" records of the investigation.

The development of inexpensive, effective microcomputers and other information technologies may be outflanking traditional, informal confidentiality protections which relied, in part, upon the inaccessibility of intelligence and investigative data held in manual, chronological and non-name indexed systems. Because any regulation of this technology, or the information entries which it records presents extraordinarily sensitive First Amendment issues, no resolution is in sight.[311]

Conclusion

Intelligence and investigative information is perhaps the most controversial type of criminal justice information. Thus, there is interest in a reference work such as this which comprehensively addresses the practice, the policies and the law as they apply to intelligence and investigative information. In so doing this report contributes to a greater understanding of intelligence and investigative information as well as to the development of consensus principles for the collection, maintenance and dissemination of this data.

FOOTNOTES

[1]Investigative information is defined in the report to mean personal information compiled in the course of an investigation of a specific criminal act. Intelligence information is defined to mean personal information compiled in an effort to anticipate, prevent or monitor possible criminal activity.

[2]SEARCH Technical Report Number 13, Standards for Security and Privacy of Criminal Justice Information, (1975), Standard 2.1(g) (Hereafter, "Technical Report 13").

[3]Id., Standard 2.1(f).

These definitions were first proposed by SEARCH in 1975. Today, many states use the SEARCH definitions in their criminal justice information statutes. For example, Indiana, Iowa (Iowa Code Ann. § 692.1), and Montana (Mont. Code Ann. § 44-5-101(5) and (6)), to name just a few, have adopted the SEARCH definitions for intelligence and investigative information.

Ind. Code Ann. § 5-2-4-1(b) defines criminal intelligence information as information on, "identifiable individuals compiled in an effort to anticipate, prevent or monitor possible criminal activity;" and criminal investigative information as information on, "identifiable individuals compiled in the course of an investigation of specific criminal acts."

The complete and official statutory citation is used in this report the first time that a particular state's statute is cited. Thereafter, statutory citations are presented simply by citing the state's name and the appropriate chapter or section numbers.

[4]Gilbert, Criminal Investigation, Charles Merrill Co. (1980), at Ch. 3 (Hereafter, "Gilbert").

[5] Dintino and Martens, Police Intelligence Systems in Crime Control, Thomas (1983) at p. 5 (Hereafter, "Dintino and Martens").

Definitions for intelligence information, in particular, have received considerable attention in the police literature. Most of that literature uses this term to mean, "information that has been processed--collected, evaluated, collated, analyzed and reported." Godfrey and Harris, Basic Elements of Intelligence, LEAA (1971), at p. 2 (Hereafter, "Godfrey and Harris"). At least one police intelligence text has defined the term intelligence in a far more operational and colorful way, as follows, "[A]n intelligence operation is simply a euphemism for spying." Bouza, Police Intelligence, The Operations of an Investigative Unit, AMS Press Inc. (1976) at p. 1, (Hereafter, "Bouza"). According to Dintino and Martens, (p. 5) the origin of the term intelligence has been traced at least to 1593 when it was used to mean "superior understanding."

[6] This definition is based on the widely accepted definition found in the Department of Justice's Criminal Justice Information Systems regulations at 28 C.F.R. § 20.3(b).

[7] Hawaii Rev. Stat. § 846-1(3); Ill. Rev. Stat. ch. 38 § 206-7; Ind. § 5-2-4-2; Indiana's statute warns that intelligence information "shall not be placed in a criminal history file nor shall a criminal history file indicate or suggest that a criminal intelligence file exists on the individual to whom the information relates;" La. Code Crim. Proc. Ann. art. 15:576; Neb. Rev. Stat. § 29-3506; Nev. Rev. Stat. § 179A. 070(2); 18 Pa. Cons. Ann. ch. 9102; and Va. Code, Ch. 27, art. 1 § 9-169.

[8] 18 Pa. ch. 91-9102.

[9] Gilbert, at p. 2.

[10] Id., at p. 3.

[11] Id.

[12] Marchand, Police Intelligence Information and Privacy; Policy Guidelines for the 1980s, Bureau of Government Research and Service, University of South Carolina (1980), at p. 7 (Hereafter, "Marchand"); and Richardson, The New York Police, Colonial Times to 1901, Oxford Univ. Press, Ch. 1 (1970) (Hereafter, "Richardson").

[13] Gilbert, at p. 3.

[14] Id.

[15] New York's original night watch, consisting of six men, was called the "rattle watch." Walling, Recollections of a New York City Chief of Police, Caxton Book Concern, (1887) at p. 29. As early as the 1790's, New York City's marshals were charged with investigative tasks. The Charge of Responsibilities authored by the Mayor of New York and sent to New York's Marshal's service in the late 1790's, included the following order: "You shall be vigilant in detecting and bringing to justice all Murderers, Robbers, Thieves and other Criminals." Richardson, at p. 18.

[16] Gilbert, at p. 14.

[17] Krajeck, "Policing Dissent: The New Limits for Surveillance," Police Magazine, Sept. 1981 at pp. 6-24.

[18] Bouza, at p. 51.

[19] Gilbert, at p. 16. Allan Pinkerton is often thought of as America's "father" of criminal investigation. He was the first detective in the Chicago Police Department in 1851. Later, his private detective agency virtually monopolized criminal intelligence work through the middle of the 19th century. The Pinkertons are credited with being the first to use infiltrators and shadowing.

[20] Donner, The Age of Surveillance, Vintage (1981), at p. 32.

[21] Draper, "Privacy and Police Intelligence Data Banks: A Proposal to Create a State Organized Crime Intelligence System and to Regulate the Use of Criminal Intelligence Information," Harv. J. Legis. 14:1 (1976) at p. 3 (Hereafter, "Harv. J.").

[22] Bouza, at p. 24.

[23] Id.

[24] Gilbert, at p. 19.

[25] Gilbert, at p. 23.

[26] Gilbert, at p. 25.

[27] Donner, at p. 33.

[28] Bouza, at p. 24. BOSSI was destined for two more name changes. In 1931 it was renamed the Bureau of Criminal Alien Investigation. In 1945, in what may be the most euphemistic moniker ever given to an intelligence unit, the organization was named the "Public Relations Squad." Mercifully, the unit was given its present name only one year later.

[29] Donner, at p. 32.

[30] Gilbert, at p. 17.

[31] Task Force Report: Organized Crime, The President's Commission on Law Enforcement and Administration of Justice 1967 at p. 10 (Hereafter, "Task Force Report").

[32] Marchand, at p. 9, and see, Ungar, The FBI, Little Brown & Co., (1975).

[33] Westin, Privacy and Freedom, Atheneum, (1967) at p. 174.

[34] Gilbert, at p. 17.

[35] Id.

[36] Id.

[37] Task Force Report, at p. 11.

[38] Id., at p. 11.

[39] Id., at p. 16.

[40] Draper, Harv. J., at p. 14.

[41] Report of the Warren Commission on the Assassination of President Kennedy, pp. 433-34; and see, "Preventative Intelligence Systems and the Courts," Calif. L. Rev. 58:914, 916 (1970).

[42] Rights in Conflict, the Official Report of the National Commission on the Causes and Prevention of Violence, Signet Books, at p. 78; and see, Davis, "Police Surveillance of Political Dissidents," Colum. Hum. Rights L. Rev. 4:101, 108 (1972).

[43] Task Force Report, at p. 20.

[44] Id.

[45] Omnibus Crime Control and Safe Streets Act, codified at 42 U.S.C. 3701, et. seq.

[46] Draper, Harv. J., at p. 13.

[47] Id., at p. 14.

[48] Hardest hit were the FBI's COINTELPRO program, which was accused of utilizing supposedly confidential income tax information to monitor and discredit or disrupt certain dissident domestic groups; the Internal Revenue Service's Special Services Staff, which was accused of serving as the IRS's political intelligence arm from 1969 to

1973; Operation CHAOS, the CIA's operation designed to monitor foreign contacts by American dissidents, but which was charged with accumulating detailed intelligence data about numerous political activists; the Army's CONUS intelligence system, which, allegedly, held files on several million domestic political activists; and finally, recently beefed up intelligence units in several big cities, including Chicago's "Blackstone Rangers" and New York's BOSSI.

Literally hundreds of magazine and newspaper articles provided detailed, and sometimes lurid, accounts of the nation's binge of domestic political intelligence activity in the late 1960's and early 1970's. Among the more acclaimed are, Pyle, "The Army Watches Civilian Politics," Washington Monthly, Jan. 1970, at p. 5; Wicker, "The Undeclared Witch-Hunt," Harper's, Nov. 1969, at p. 109; and Lundy, "The Invisible Police," The Nation, Dec. 8, 1969, at p. 629.

[49]Bouza, at p. 1.

[50]See, for example, "Hearings on Federal Data Banks, Computers and the Bill of Rights," before the Subcommittee on Constitutional Rights of the Senate Comm't on the Judiciary, 92nd Cong., 1st Sess. (1971); "Hearings on Criminal Justice Data Banks," before the Subcommittee on Constitutional Rights of the Senate Comm't on the Judiciary, 93rd Cong., 2d Sess. (1974); "Hearings on Military Surveillance," before the Subcommittee on Constitutional Rights of the Senate Comm't on the Judiciary, 93rd Cong., 2d Sess. (1974); and, for a summary of these and other hearings held by the Senate and House on the subject of domestic intelligence activity, see "Hearings on Surveillance Technology: Policy and Implications," Report of the Subcommittee on Constitutional Rights of the Senate Comm't on the Judiciary, 94th Cong., 2d Sess. (1976), at pp. 111-133.

[51]For example, H.R.136, 92d Cong., 1st Sess. (1971) would have restricted military domestic intelligence; S.2542,

93rd Cong., 2d Sess. (1974) would have placed restrictions on state and local agency collection and dissemination of intelligence and investigative information; and S.2008, 94th Cong., 1st Sess. (1975) also would have restricted state and local collection and dissemination of intelligence and investigative data.

[52]FBI Guidelines for Domestic Security Investigations, published by Attorney General Levi on March 10, 1976.

[53]43 Fed. Reg. 28572, June 30, 1978, and subsequently revised at 45 Fed. Reg. 61613, Sept. 17, 1980 and 28 C.F.R. § 23.

[54]See, "The Erosion of Law Enforcement Intelligence and its Impact on Public Security," before the Subcomm't on Criminal Laws and Procedures of the Senate Comm't on the Judiciary, 95th Cong. 1st Sess. (Sept. 1977).

[55]The "Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations," March 7, 1983.

[56]S.774, 98th Cong., 2d Sess. (1984).

[57]Bouza, at p. 59; "Anderson v. Sills: The Constitutionality of Police Intelligence Gathering." N.W.U.L. Rev., 1970, at p. 463 (hereafter "N.W.U.L. Rev."); and see, Appendix A to the opinion in Anderson v. Sills, 106 N.J. Super. 545, 558 (Ch. Div. 1969).

[58]One criminal investigations textbook urges investigators to collect the following information about suspects: "sex, race, coloring, age, height, weight, hair (color, style, condition), eyes (color, size, glasses), nose (size and shape), ears (close to head or protruding), distinctive features (birthmarks, scars, beard), clothing, voice (high or low, accent), other distinctive characteristics such as walk." Bennett & Hess, Criminal Investigation, West Publishing (1981), at p. 207; and see, Gilbert, at p. 64.

[59]Tulley, CIA: The Inside Story, William Morrow (1962) at p. 85; and see, Bouza, at p. 47.

[60]507 F.2d 1116, 1126 (D.C. Cir. 1974).

[61]Gilbert, at p. 55-61; and see, Simi Valley Police Department, Policy and Procedures Manual, Managing Criminal Investigations, Gen. Order 0814, 9/1/81. (Hereafter, "Simi Valley Police Department").

[62]Simi Valley Police Department, at p. 1.

[63]Wolf, The Police Intelligence System, John Jay Press (1975), at p. 8 (Hereafter, "Wolf"). See also, Task Force Report, at p. 12.

[64]For a period in the early 1970's, for example, one police department in the Southeast reportedly, used a minicomputer to examine the records of many local real estate transactions. The examination identified the names of hundreds of individuals active in the local real estate market. When this list was matched against a list of people involved in activities of police interest (such as loan sharking), the "hits," or matches, identified people who might be involved in various real estate frauds. Draper, Harv. J., at p. 16.

[65]Gilbert, at p. 39.

[66]Skousen, "The Intelligence Unit," Law and Order, (June 1966) at p. 68.

[67]Bouza, at p. 45; and see, Cahill, "Intelligence Unit is a Key Division of a Police Agency," FBI Law Enforcement Bulletin, (Sept. 1962), at p. 15.

[68]Bouza, at p. 19.

[69]Simi Valley Police Department, at p. 1.

[70]Gilbert, at p. 39.

[71]Id.

[72]Supra, note 7.

[73]Godfrey, at p. 6.

[74]Id.

[75]Gilbert, at p. 71.

[76]Draper, Harv. J., at pp. 13-14.

[77]Godfrey, at p. 6; and Bonza, at p. 150.

[78]Godfrey, at p. 38.

[79]Id., and Bouza, at p. 45.

[80]One criminal intelligence agency defined its mission, for instance, as follows: "to obtain information relating to the political or social activities of any person or group, which are likely to result in a crime or serious problem for the police." Bouza, at p. 19.

[81]Godfrey, at p. 6.

[82]Bouza, at p. 46.

[83]Wolf, at p. 17.

[84]Id.

[85]These agencies include the FBI; the Secret Service; the Drug Enforcemnt Agency; the U.S. Marshals; the Alcohol, Tobacco and Firearms Bureau; the Federal Aviation Administration; the Internal Revenue Service; the Customs Bureau; the Immigration and Naturalization Service; and the Postal Service. Report of the Comptroller General,

"The Multi-State Regional Intelligence Projects--Who Will Oversee These Federally Funded Networks" (1980). (Hereafter, "GAO Report")

[86]Wolf, at p. 8.

[87]Some urban criminal intelligence agencies, for example, have indexed their intelligence files by name, class of crime, area of crime and business. Draper, Harv. J., at p. 11.

[88]The Law Enforcement Intelligence Unit ("LEIU") is an informal affiliation of criminal intelligence units and officers throughout the country.

According to some reports, LEIU maintains a name index of 20,000 alleged organized crime figures who are the subject of intelligence files held by member organizations. Authorized participants can query this index to locate relevant files, and participating agencies are expected to share data with authorized requestors. Privacy Journal, (Feb. 1979) at p. 6.

In addition, many state and local criminal justice agencies participate in one of the federally funded regional intelligence information systems. These systems include: the Regional Organized Crime Information Center ("ROCIC"), operating in 14 southeastern states; the Rocky Mountain Information Network ("RMIN"); the New England State Police Administrators Conference ("NESPAC"); the Mid-States Organized Crime Information Center ("MOCIC"); the Mid-Atlantic-Great Lakes Organized Crime Law Enforcement Network ("MAGLOCLEN"); and LEVITICUS, consisting of four southern coal producing states, plus New York, Pennsylvania and Virginia.

Many of these systems focus principally on organized criminal activity involving narcotics violations. In general, the systems operate, or are planning to operate, name indexes to intelligence information about individuals held by member agencies. None of the systems permits access to their data by non-member organizations.

[89]Godfrey, at p. 108.

[90]Ill. Ann. Stat. Ch. 127, § 55a(5)(a); and see, Draper, Harv. J., at p. 31.

[91]Boyd v. United States, 116 U.S. 616 (1886).

[92]Fisher v. United States, 425 U.S. 391 (1976).

[93]18 U.S.C. § 2510 et. seq.

[94]42 U.S.C. § 2000 aa.

[95]12 U.S.C. § 3401 et. seq.

[96]28 C.F.R. § 23.20(a).

[97]1983 Domestic Security Guidelines, Sec. III. B.1.

[98]Seattle City Ordinance No. 108333; and see, SEARCH Issue Brief No. 2.

[99]Ind. § 5-2-4-3.

[100]S. 2008, "The Criminal Justice Information Control and Protection of Privacy Act of 1975," 94th Cong., 1st Sess., defines "criminal justice intelligence information" to mean information associated with an identifiable individual compiled by a criminal justice agency in the course of conducting an investigation of an individual relating to possible future criminal activity of an individual, or relating to the reliability of such information, including information derived from reports of informants, investigators or from any type of surveillance."

[101]Id., at § 210(b).

[102]Draper, Harv. J., at p. 31; and see, 121 Cong. Rec., at p. 11554 (1975).

[103]New York City Council Bill, Intro. No. 780; Bouza, at p. 161.

[104]Some of the regional intelligence systems are restricted to looking only, or primarily, at suspected narcotics violators.

[105]5 U.S.C. § 552(b)(7).

[106]See, for example, Pratt v. Webster, 673 F.2d 408, 421 (D.C. Cir. 1982); and Moorefield v. U.S. Secret Service, 611 F.2d 1021, 1025 (8th Cir. 1980) cert. denied, 449 U.S. 909.

[107]5 U.S.C. § 552a(e)(7).

[108]O'Reilly, Federal Information Disclosure, Shepard's (1983) at § 2206.

[109]Id., and see 120 Cong. Rec. 40881 (Dec. 18, 1974). The Privacy Act states that federal agencies shall "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;" 5 U.S.C. § 552a(e)(7).

[110]American Federation of Government Employees, Local 421 v. Schlesinger, 443 F. Supp. 431, 435 (D.D.C. 1978).

[111]Albright v. United States, 631 F.2d 915, 919 (D.C. Cir. 1980).

[112]Privacy Journal, Compilation of State Privacy Laws, (1981).

[113]Ind. § 5-2-4-5.

[114]256 A.2d 298, 305 (N.J. Sup. Ct., Chancery Div., 1969).

[115]NAACP v. Alabama, 357 U.S. 449, 460 (1958).

[116]See, for example, "Preventative Intelligence Systems and the Courts," Calif. L. Rev. 58:914 (1970); Davis, "Police Surveillance of Political Dissidents," Colum. Hum. R.L. Rev. 4:101 (1972); Askin, "Police Dossiers and Emerging Principles of First Amendment Adjudication," Stan. L. Rev. 22:196 (Jan. 1970); "Anderson v. Sills: the Confidentiality of Police Intelligence Gathering," N.W.U.L. Rev. 461 (1970); "Secret Files: Legitimate Police Activity or Unconstitutional Restraint on Dissent?", Georgetown L.J. 58:569 (1970); "Political Surveillance and Police Intelligence Gathering--Rights, Wrongs and Remedies," Wisc. L. Rev. 1972; 175 (1972).

By 1971, one commentator counted nearly twenty law suits supported by the ACLU, alone, in which plaintiffs were seeking relief under the Anderson chilling effect theory, from intelligence systems operated by the FBI, the Army and state and local police departments. Davis "Police Surveillance of Political Dissidents," Colum. Hum. R. L. Rev. 4: 101 at p. 109 (1972).

[117]In Board v. State Bar of Arizona, 401 U.S.1 4-5 (1971) the plaintiff had been denied admission to the bar solely because of her refusal to answer a question regarding past organizational associations; in Keyshian v. Board of Regents, 385 U.S. 589, 592 (1967), teachers were threatened with discharge because of their political acts; in Bagget v. Bullitt, 377 U.S. 360 (1967), the plaintiff was required to take an oath as a condition of employment in a government agency; and, of course, in NAACP the plaintiff's were the "victims" of a compulsory reporting order.

[118]408 U.S. 1, 11 (1972).

[119]Laird v. Tatum, 408 U.S. 1, 11 (1972).

[120]See, Halkin v. Helms, 690 F.2d, 977, 1002 (D.C. Cir. 1982); and see, Schlesinger v. Reservists Comm't to Stop the War, 418 U.S. 208, 220-21 (1974).

[121] 28 C.F.R. § 23.20(g).

[122] Wolf, at p. 20.

[123] Federal Records Act, 44 U.S.C. Ch. 21.

[124] Alaska Stat. § 6AA C60.110.

[125] Ind. § 5-2-4-4.

[126] See, SEARCH, Technical Report No. 27, Sealing and Purging of Criminal History Record Information, (April 1981), at p. 13.

[127] S.2008, § 210(b).

[128] S.2008, § 211(a).

[129] Walker v. Lamb, 254 A.2d 265, 266 (Del. 1969).

[130] 473 F.2d 180, 185 (D.C. Cir. 1972).

[131] 550 SW.2d 799, 803 (Mo. 1977).

[132] 524 F.2d 862, 868 (3rd Cir. 1975).

[133] Id. at p. 869.

[134] 401 F. Supp. 706, 716 (E.D. Wisc. 1975).

[135] See, Federal Information Disclosure, at § 17.07.

[136] Id. at § 17.04.

[137] Iowa § 692.8.

[138] 18 Pa. § 9106.

[139] 28 C.F.R. § 23.20(h)(i)(2).

[140] La. § 1-18:9(3)(4).

[141] Wolf, at p. 23.

[142] 5 U.S.C. § 552a(e).

[143] 5 U.S.C. § 552a(j).

[144] 28 C.F.R. § 23.20(f).

[145] Carroll, Confidential Information Sources: Public and Private, Security World Publishing Co. (1975) at p. 120.

[146] Privacy and Security of Criminal History Information: Privacy and the Media, U.S. Department of Justice, (1979) at p. 32 (Hereafter, "Privacy and the Media").

[147] "National Security, Law Enforcement, and Business Secrets under the Freedom of Information Act." The Business Lawyer, 38:707 (Feb. 1983) (Hereafter, "Business Lawyer").

[148] Id.

[149] See, Privacy and the Media, at p. 31.

[150] Attorney General's Memorandum on the 1974 Amendments to the Freedom of Information Act at p. 8 (1975).

[151] Privacy and the Media at p. 32.

[152] Alaska Stat. § 12.62.015.

[153] Ind. Stat. Ann. § 5-2-4-6.

[154] Iowa Code Ann. § 692.8.

[155] La. Rev. Stat. Ann. § 44:3-B (barring disclosure of records that would tend to impart the identity of a confidential source).

[156] Me. Rev. Stat. Ann. § 16-614.

[157] Mont. § 44-5-303.

[158] N.J. Rev. Stat. Ann. § 53:6-18.

[159] Tenn. Code Ann. § 10-7-504.

[160] Wyo. Stat. § 9-1-627(c).

[161] Ind. Stat. Ann. § 5-2-4-6.

[162] Mont. Code. Ann. § 44-5-303.

[163] Alaska Stat. § 12.62.030.

[164] Ariz. Rev. Stat. Ann. tit. 13, § 1273.

[165] Ark. Stat. Ann. § 12-2803.

[166] Ill. Stat. Ann. Ch. 38, § 206-7.

[167] Mass. Gen. Laws Ann. § 6-172.

[168] Okla. Stat. Ann. tit. 47 § 2-129.

[169] Wash. Rev. Code Ann. § 43.43.856.

[170] 28 C.F.R. § 23.20(d).

[171] 28 C.F.R. § 23.20(e).

[172] S.2008, § 210(d).

[173] S.2008, §211(c).

[174] Attorney General's Guidelines, at Sec. V.

[175] Draper, Harv. J., at pp. 37-38.

[176] In Colucci v. Chicago Crime Comm., 334 N.E.2d 461, 470 (Ill. 1975), for example, a court held that calling a person an "organized crime figure" is defamatory.

[177] See, Nelson v. Eastern Airlines, 24 A.2d 371, 378 (N.J. 1942); and see, Annot. "Liability of Police or other Peace Officers for Defamation" 13 ALR 2d 897, 901. (Hereafter, "13 A.L.R.2d 897").

[178] In Melvin v. Reid, 112 Cal. App. 285, (1931), the court said that disclosure of a woman's earlier career as a prostitute is the kind of "private fact" covered by this doctrine.

Although intelligence and investigative information is seldom characterized as public record information, an Oregon court, Ayers v. Lee Enterprises, Inc., 561 P.2d 998, 1002 (Ore. 1977) held that a police department's release of a rape victim's name from a police report was not actionable because, under then-existing Oregon law, the name and address of the victim of any "infamous name" was a public record.

Of course, once a victim testifies in a trial or other public proceeding, any identification information or other information presented in the proceeding is a matter of public record, absent a gag order, and publication of this information does not expose the newspaper or other party to an invasion of privacy action. Poteet v. Roswell Daily Record, 584 P.2d 1310, 1312 (N.M. 1978).

[179] Prosser, Torts at p. 823 (West's 3rd Ed.).

[180] 13 ALR 2d 897, 899.

[181] Id., and see, In re Catron v. Jasper, 198 So.2d 322, 325 (Kent. 1946), in which a Kentucky state court held that the disclosure by a sheriff to his deputy that the plaintiff

was selling liquor illegally was absolutely privileged in view of the local sheriff's duty to enforce the law.

[182]See, Munn v. Burks, 526 P.2d 1040, 1041 (Ore. 1974); Shade v. Bowers, 199 N.E.2d 131, 139 (Ohio 1962), both holding that law enforcement officials are absolutely privileged to disclose intelligence information to liquor control commissions.

[183]For a fuller discussion of the standards for liability and damages involving both federal and state criminal justice officials, see SEARCH, Liability for Mishandling Criminal Records (1984).

[184]261 F. Supp. 570, 574 (D. Md. 1966).

[185]389 F. Supp. 529, 538 (D.D.C. 1975).

[186]Id., at p. 537.

[187]Id.

[188]436 P.2d 613, 620 (Ariz. 1968).

[189]Id., at p. 619.

[190]Id., citing, Missouri Pacific Railway Co. v. Richmond, 11 S.W.555, 557-558 (Tex. 1889); and see also, Morton v. Knipe 112 N.Y.S. 451, 452-453 (1908) holding that a police officer is not liable for disclosing to a landlord that the landlord's tenant was under investigation for operating a house of prostitution.

[191]637 S.W. 2d 251, 255 (Mo., 1982).

[192]Tarlton v. Saxbe, 507 F.2d 1116, 1117 (D.C. Cir. 1974); this duty can also be based on common law negligence theories, and its violation can thus result in a civil suit for damages under a variety of common law tort theories. See, for example, Testa v. Wingquist, 451 F. Supp. 388, 394 (D.R.I. 1978).

[193]See, SEARCH, Liability for Mishandling Criminal Records (1984) at p. 26.

[194]In Menard v. Mitchell, 430 F.2d 486, 491 (D.C. Cir. 1970), for example, the court held that where an arrest ends in a favorable disposition the record subject may have a constitutionally based claim to limit the dissemination of that arrest record.

[195]424 U.S. 693, 713 (1976).

[196]5 U.S.C. § 552(a)(1)-(3). The FOIA does not define the term "records." Case law indicates that an agency's possession, control and use of written material makes this material an agency record for FOIA purposes. See, Forsham v. Harris, 445 U.S. 169, 186, n. 17 (1980); Kissinger v. Reporters Committee for Freedom of the Press, 445 U.S. 136, 155, 157 (1980); and Federal Trade Commission v. Anderson, 631 F.2d 741, 748-750 (D.C. Cir. 1979).

[197]5 U.S.C. § 552(b)(7).

[198]Chrysler v. Brown, 441 U.S. 281, 292-293 (1979).

[199]5 U.S.C. § 552a(b).

[200]See, for example, Jensen v. Schiffman, 544 P.2d 1048, 1051 (Ore. 1976).

[201]See, the chart, entitled State Investigatory Record Exemptions, in Chapter Five. The chart identifies exemptions which cover investigative and intelligence information.

[202]Los Angeles Police Dept. v. Superior Court of Los Angeles, 65 Cal. App. 3d 661, 668 (Cal. 1977).

[203]487 F. Supp. 127, 131 (N.D. Calif. 1979).

[204] Id. at p. 131.

[205] See, Annot., "What Constitutes Investigatory Files Exempt from Disclosure Under Freedom of Information Act," 17 ALR Fed. 522; and, Annot., "What are Enforcement Proceedings Within Freedom of Information Act Exemption From Disclosure of Investigatory Records that would Interfere with Enforcement Proceedings," 55 ALR Fed. 583.

[206] The Attorney General's Memorandum on the 1974 Amendments to the Freedom of Information Act, at p. 6 (Hereafter, "Attorney General's Memorandum").

[207] Federal Information Disclosure, at pp. 17-20.

[208] Nationwide Mutual Ins. Co. v. Friedman, 451 F. Supp. 736, 741-742 (D.Md. 1978).

[209] Bristol-Meyers Co. v. FTC, No. 77-1275 (D.C. Cir. 1978); and see, Federal Information Disclosure, at pp. 17-20.

[210] 565 F.2d 692, 696 (D.C. Cir. 1977); and see, Stern v. Richardson, 367 F. Supp. 1316, 1321 (D.D.C. 1973). However, information compiled in the FBI's COINTELPRO investigation was found to be covered by the investigatory records exemption. Pratt v. Webster, 673 F.2d 408, 423 (D.C. Cir. 1982).

[211] See, Agee v. Central Intelligence Agency, 517 F. Supp. 1335, 1339 (D.D.C. 1981).

[212] Federal Bureau of Investigation v. Abramson, 456 U.S. 615, 102 S.Ct. 2054, 2064 (1982).

[213] National Labor Relations Board v. Robbins Tire and Rubber Co., 437 U.S. 214, 232 (1978).

[214] The Attorney General's Memorandum cites legislative history indicating that the courts should construe the exemption flexibly to ensure that none of the harms set out in the exemption occurs, at p. 8. Thus far, many courts have done so. For example, in National Public Radio v. Bell, 431 F. Supp. 509, 514 (D.D.C. 1977), the Department of Justice conceded that its investigation was in a dormant stage in that all available leads had been pursued and the Department had no funds to pursue the investigation further. Nevertheless, the court held that 7(A) was available so long as the possibility of future law enforcement action existed.

[215] 611 F.2d 1021, 1025 (8th Cir. 1980).

[216] Exemption 7(B) permits the withholding of investigatory records where disclosure would "deprive a person of a right to a fair trial or an impartial adjudication." This exemption is principally concerned with protection of the record subject's fair trial interests from prejudicial publicity. Attorney General's Memorandum at pp. 8-9. Once an investigation or proceeding is closed this exemption is not germane.

[217] National Labor Relations Board v. Robbins Tire and Rubber Co., 437 U.S. 214, 231-232 (1978).

[218] 5 U.S.C. § 552(b).

[219] Robbins Tire and Rubber, at p. 224.

[220] Associated Dry Goods Corp. v. National Labor Relations Board, 455 F. Supp. 802, 814-15 (S.D. N.Y. 1978).

[221] Department of the Air Force v. Rose, 425 U.S. 352, 378 n. 16 (1976).

[222] Common Cause v. Ruff, 467 F. Supp. 941, 942 (D.D.C. 1979).

[223] See, for example, Dunaway v. Webster, 519 F. Supp. 1059, 1079 (N.D. Calif. 1981).

[224] Fund for Constitutional Government v. National Archives and Records Service, 485 F. Supp. 1, 8 (D.D.C. 1978) (release of records of Watergate Special Prosecution Force regarding alleged wrongdoing in connection with corporate campaign contributions, in the absence of criminal charges, would subject individuals to public embarrassment and ridicule); Baez v. Department of Justice, 647 F.2d 1328, 1338 (D.C. Cir. 1980), ("to release the identities of these individuals and the information collected about them . . . would announce to the world that those individuals were targets of an FBI investigation. There can be no clearer example of an unwarranted invasion of privacy than to release to the public that another individual was the subject of an FBI investigation"); Cerveny v. Central Intelligence Agency, 445 F. Supp. 772, 776 (D. Colo. 1978) (unsubstantiated personal information which is derogatory would not be disclosed from CIA intelligence files because its disclosure would violate the subject's privacy interests); C.F. Antonelli v. Federal Bureau of Investigation, 536 F. Supp. 568, 574, 575 (N.D. Ill. 1982), (holding that FOIA exemption was not satisfied by FBI affidavit asserting that admitting existence of FBI file alone would constitute an unwarranted invasion of privacy).

[225] Demetracopoulos v. Federal Bureau of Investigation, 510 F. Supp. 529, 533 (D.D.C. 1981).

[226] Librach v. Federal Bureau of Investigation, 587 F.2d 372, 373 (8th Cir. 1978).

[227] Malizia v. United States Dept. of Justice, 519 F. Supp. 338, 348 (S.D. N.Y. 1981).

[228] Committee on Masonic Homes of the R.W. Grand Lodge F and AM of Penn v. National Labor Relations Board, 414 F. Supp. 426, 431 (E.D. Pa. 1976), vacated and remanded on other grounds, 556 F.2d 214 (3rd Cir. 1977).

Several Exemption 6 decisions have identified the kind of intimate, personal information protected by that exemption (and thus presumably protected by 7(C)). In Rural Housing Alliance v. United States Dept. of Agriculture, 498 F.2d 73, 77 (D.C. Cir. 1974), rehearing denied, 502 F.2d 1179, marital status, legitimacy of children, medical conditions and welfare payments were considered protectible; and in Robles v. Environmental Protection Agency, 484 F.2d 843, 845 (4th Cir. 1973), intimate details of a highly personal nature in an individual's employment record or health history were considered protectible.

[229] Associated Dry Goods Corp. v. National Labor Relations Board, 455 F. Supp. 802, 815 (S.D. N.Y. 1978).

[230] Title Guarantee Co. v. National Labor Relations Board, 534 F.2d 484, 489, n. 10 (2nd Cir. 1976), and cases cited therein.

[231] 516 F. Supp. 145, 149 (D.D.C. 1980).

[232] 627 F.2d 392, 399 (D.C. Cir. 1980).

[233] Tarnopol v. Federal Bureau of Investigation, 442 F. Supp. 5, 8 (D.D.C. 1977) (Personal curiosity will not establish a public interest necessary to justify release of FBI investigatory records); Wine Hobby U.S.A., Inc. v. Internal Revenue Service, 502 F.2d 133, 137 (3rd Cir. 1974) (IRS would not release the names of individuals registered to produce wine at home where the requestor's purpose was merely "commercial exploitation").

[234] 403 F. Supp. 1318, 1321 (M.D. Tenn. 1975).

[235] Hatch, "Too Much Freedom Under FOIA," Am. Bar Assoc. J, at p. 556, (May, 1983).

[236] Id., see also, "National Security, Law Enforcement and Business Secrets Under the Freedom of Information Act," The Business Lawyer 38:707 (Feb. 1983).

[237]S.774 states that the FOIA's disclosure provisions shall not apply to an "informant's records maintained by a law enforcement agency under an informant's name or personal identifier, whenever access to such records is sought by a third party according to the informant's name or personal identifier."

[238]519 F. Supp. 1059, 1081 (D.D.C. 1981).

[239]Id. at p. 1081; and see, Malloy v. Dept. of Justice, 457 F. Supp. 543, 546 (D.D.C. 1978).

[240]Lamont v. Department of Justice, 475 F. Supp. 761, 780 (S.D. N.Y. 1979).

[241]Schauer v. Bell, 433 F. Supp. 438, 441 (N.D. Ga. 1977).

[242]See, Northern Calif. Police Practices Project v. Craig, 90 Cal. App. 3d 116, 120-121 (1979); Cook v. Craig, 55 Cal. App. 3d 773, 783, (Cal. 1976). See also, chart in Appendix A.

[243]Conn. Gen. Stat. Ann. § 1-19(b).

[244]D.C. Code Ann. § 1-1524(a)(3).

[245]La. Rev. Stat. Ann. §§ 44:3-A and 44:3-B.

[246]Md. Ann. Code of 1957 art. 76A, § 3(i).

[247]Mich. Stat. Ann. § 4.1801(13)(1)(b).

[248]S.C. Code Ann. § 30-4-40(3).

[249]Ky. Rev. Stat. § 17.150(2).

[250]Me. Rev. Stat. Ann. § 16-614.

[251]N.Y. Pub. Off. Law art. 6, § 87(2)(e).

[252]Cal. Gov't Code § 6254(f).

[253]Del. Code Ann. 29 § 29-10002(d).

[254]Mass. Gen. Laws Ann. ch. 4, § 7(f).

[255]Minn. Stat. Ann. § 13.82(5).

[256]Neb. Rev. Stat., § 84-712.05(5).

[257]Or. Rev. Stat. Ann. § 192.500(1)(c).

[258]Pa. Stat. Ann. tit. 65, § 66.1(2).

[259]R.I. Gen. Laws § 38-2-2(d)(4).

[260]Vt. Stat. Ann. tit. 1, Ch. 5 § 317(b)(5).

[261]Mass. Gen. Laws Ann. Ch. 4, § 7(f).

[262]Bongas v. Chief of Police of Lexington, 354 N.E.2d 872, 876 (Mass. 1976); C.F., Reinstein v. Police Commissioner of Boston, 391 N.E. 2d 881, 885 (Mass. 1979).

[263]Del. Code Ann. § 10002(d)(5).

[264]Minn. Stat. Ann. § 13.82(5).

[265]Op. Atty Gen. No. I80-45.

[266]130 Ariz. 415, 636 P.2d 663.

[267]Brown v. Minter, 254 S.E. 2d 326, 327 (1979).

[268]Minn. Stat. Ann. § 13.82(5).

[269]237 Ga. 764, 229 S.E.2d 624, (Ga. 1976).

[270]See, 28 C.F.R. § 20.

[271] See, generally, The Report of the Privacy Protection Study Commission (1977) at p. 17.

[272] 369 A.2d 558, 562 (Md. 1977).

[273] 497 F. Supp. 209, 211, 212 (S.D.N.Y. 1980).

[274] 391 N.Y.S.2d 953, 954 (Sup. Ct. 1977). See also, Lamont v. Department of Justice, 475 F. Supp. 761, 775 (S.D.N.Y. 1979).

[275] 5 U.S.C. § 552a(d), and see, Privacy Journal, Compilation of State Privacy Laws, (1981).

[276] 5 U.S.C. § 552a(j) and (k).

[277] Los Angeles Police Dept. v. Superior Court of Los Angeles, 135 Cal. Rptr. 575 579 (Cal. 1977).

[278] See, State v. Hall, 218 So.2d 320, 322 (La. 1969); Nakagawa v. Heen, 568 P.2d 508, 511 (Ha. 1977); Pitchess v. Superior Court of Los Angeles, 522 P.2d 305, 307 (Cal. 1974); Tighe v. City and County of Honolulu, 520 P.2d 1345, 1348 (Ha. 1974).

[279] Nerov v. Hyland, 368 A.2d 965, 966 (N.J. 1977).

[280] Martinelli v. Dist. Court in and for City and County of Denver, 612 P.2d 1083, 1089 (Colo. 1980).

[281] In People v. Wilkens, 287 P.2d 555, 559 (Cal. 1955), the court rejected, on privacy grounds, a discovery request by defendants charged with pandering for information pertaining to persons who had admitted to being arrested for activities related to prostitution.

For a full discussion of litigant access cases, see, Annot., "Validity, Construction, and Application of Statutory Provisions Relating to Public Access to Police Records," 82 ALR3d 19 at p. 45 (Hereafter "Public Access to Police Records").

[282] See, "Public Access to Police Records" at § 18.

[283] Cox v. Cohn, 430 U.S. 469, 495 (1975), upholding the press' First Amendment, right to publish the name of a rape victim once the victim's name was placed in a public court record; and see, WXYZ Inc. v. Hand, 658 F.2d 420, 427 (6th Cir. 1981), C.F. State v. Eugene, 33 N.W.2d 305, 310 (Wisc. 1948).

[284] Pell v. Procunier, 417 U.S. 817, 834-5 (1974); Branzburg v. Hayes, 408 U.S. 665, 684 (1972).

[285] In re Midland Pub. Co. v. District Court Judge, 317 N.W.2d 284, 287 (Mich. 1982).

[286] 117 Cal. Rptr. 106, 112 (1974).

[287] And, see, Annot. "Public Access to Police Records," at p. 38.

[288] 536 S.W.2d 559, 561 (Tex. 1975).

[289] 660 P.2d 785, 794 (Wyo. 1983).

[290] Id., at p. 795.

[291] Criminal Justice Information Policy: Privacy and the Private Employer, Department of Justice (1981), at p. 12.

[292] Brown v. Port of Newport, Civ. No. 74-82 (D. Ore. 1975), and see, Draper, Harv. J., at p. 26, n. 100.

[293] 341 U.S. 123, 175 (1951).

[294] N.W.U.L. Rev., at p. 474.

[295] 5 U.S.C. § 552a(a)(5).

[296] Privacy Commission Report at p. 572 et seq.

[297]See, Memorandum for William H. Webster from William French Smith, re Attorney General's Guidelines on Domestic Security/Terrorism Investigations, March 7, 1983 at p. 1.

[298]Id., at p. 7.

[299]Bouza, at p. 59.

[300]Attorney General's Guidelines on Domestic Security/Terrorism Investigations, Mar. 7, 1983.

[301]5 U.S.C. § 552a(e)(7).

[302]Bouza, at p. 59.

[303]Westin and Baker, Data Banks in a Free Society, at pp. 381-382.

[304]Privacy and the Media, at p. 32.

[305]Houston Chronicle, at p. 561.

[306]Privacy and the Media, at p. 33.

[307]See, Statement of Jonathan C. Rose, Assistant Attorney General, Office of Legal Policy before the Committee on the Judiciary, Subcommittee on the Constitution, United States Senate, concerning, S.774 on April 18, 1983; and see also S.1730.

[308]SEARCH, Case Law Digest, (1981) at p. 43.

[309]GAO Report, at pp. 19-20.

[310]Technology and Privacy, Appendix Five to the Report of the Privacy Protection Study Commission, (1977) p. 27.

[311]C.F., New Bedford Standard-Times Publishing Co. v. Clerk of the Third District Court of Bristol, 387 N.E.2d 110, 115-116 (Mass. 1979).

APPENDIX A

STATE FREEDOM OF INFORMATION STATUTES

STATE FREEDOM OF INFORMATION STATUTES

Following is a list, by state, of public records laws and a discussion of the nature of the exemption for investigative and intelligence information.

Alabama
Ala. Code tit. 41, ch. 13, §§ 1 to 44 (1982)

Public records law contains no express exemption for I&I records.* Another statute, Ala. Code. tit. 41, ch. 9, art. 23, §§ 41-9-591, et seq, establishes a criminal justice information commission as a central location for storage and dissemination of information related to crime. Sec. 41-9-636 provides that dissemination of such information shall be limited by constitutional guarantees, including privacy rights. Under § 41-9-639, "Information in a criminal history, other than physical and identifying data, shall be limited to those offenses in which a conviction was obtained or to data relating to the current cycle of criminal justice administration if the subject has not yet completed that cycle." Under § 41-9-641, the Commission is prohibited from disseminating information to out-of-state criminal justice agencies unless it pertains to a conviction.

Alaska
Alaska Stat. tit. 9, ch. 25, § 9.25.110

Public records law contains no express exemption for I&I records but provides that any records may be exempt under other statutes. Tit. 12, ch. 62, § 12.62.010 authorizes the Governor's Commission on Administration of Justice to establish rules and procedures regulating the exchange of criminal justice information. Sec.

*The abbreviation "I&I" means investigative and intelligence information as that phrase is used in this report.

12.62.015(b) provides that the commission is to establish standards for the confidentiality and security of intelligence information and provide for controls on "access to and dissemination of intelligence information, and methods for updating, correcting and purging intelligence information . . . ." Under § 12.62.030, "access to specified classes of criminal justice information systems is available only to individual law enforcement agencies according to the specific needs of the agency," and to "qualified persons" for research as well as persons inspecting records related to themselves.

Arizona
Ariz. Rev. Stat. Ann. tit. 39, §§ 121.01 to 121.02

Public records law contains no express exemption for I&I records. Tit. 13, § 1273 provides that certain criminal identification information shall be available only to law enforcement officers. The attorney general has said investigative reports need not be released to the public upon request. Instead, the information should be "carefully scrutinized" and withheld if it is confidential or if disclosure would be detrimental to state interests. Op. Atty. Gen. No. I80-45. The attorney general also has said a city police department may refuse access to information if disclosure would hinder an ongoing investigation. Op. Atty. Gen. No. I79-296. In Little v. Gilkinson, 636 P.2d 663 (Ariz. Ct. App. 1981), the court said the test for nondisclosure of investigative material is whether it would have important and harmful effects on the official duties of the agency.

Arkansas
Ark. Stat. Ann. tit. 12, ch. 28, §§ 2801 to 2806

Public records law contains no express exemption but some records may be exempt as "confidential" under § 2803, which prohibits providing to private individuals or organizations information "of a personal nature" if the

public disclosure "would constitute a clearly unwarranted invasion of personal privacy."

California
Cal. Gov't Code §§ 6251 to 6259 (West)

Public records law contains express exemption for investigative records. Such records need not be disclosed under § 6254(f), except that the names of persons involved in an incident and witnesses (other than confidential informants) shall be disclosed by local police agencies to persons involved in the incident and insurance carriers, unless disclosure would endanger an investigation.

Colorado
Colo. Rev. Stat. tit. 24, art. 72, §§ 201 to 309

Tit. 24, art. 72, §§ 301 to 305 require access to "criminal justice records" unless it is not in the public interest or unless otherwise provided by law. Tit. 24, art. 72, § 305(5) permits withholding of investigative and intelligence records on "public interest" grounds.

Connecticut
Conn. Gen. Stat. Ann., tit. 1, ch. 3, §§ 1-7 to 1-21K

Public records law exempts records of law enforcement agencies compiled to detect or investigate crime unless the information would reveal: (A) an informant's identity, (B) information prejudicial to a prospective law enforcement action, (C) investigative techniques or (D) juvenile arrest records. Tit. 1, ch. 3, § 1-19(b)(3).

Delaware
Del. Code Ann. tit. 29, §§ 10001 to 10005

Public records law exempts investigative files compiled for criminal or civil purposes. § 10002(d)(3). Intelligence files may be withheld if disclosure would endanger local, state or national welfare or security. § 10002(d)(5).

District of Columbia
D.C. Code Ann. Tit. 1, subch. II, §§ 1-1521 to 1-1527

Sec. 1-1524(a)(3) substantively duplicates federal law, exempting investigative records to the extent that disclosure would: (A) interfere with enforcement proceedings, (B) deprive a person of a right to a fair trial or impartial adjudication, (C) constitute an unwarranted invasion of personal privacy, (D) disclose the identity of a confidential source and, in some cases, confidential information provided by a confidential source, (E) disclose investigative techniques or (F) endanger the life or physical safety of law enforcement personnel.

Florida
Fla. Stat. Ann. tit. 10, ch. 119, §§ 119.01 to 119.12

Sec. 119.07(3) exempts "active" criminal I&I information as well as any information that reveals the identity of a confidential informant or surveillance techniques or surveillance personnel. The section also exempts I&I information disclosing the identity of a sex crime or child abuse victim or the assets of a crime victim, as well as any I&I information obtained before Jan. 25, 1979.

Georgia
Ga. Code ch. 40-27 §§ 40-2701 to 40-2705

Public records law contains no express exemption for I&I records but provides that any records may be exempt under other statutes. The rules of the Georgia Crime Information Center Council, ch. 140-2, § 140-2.02(c)(2) prohibit disclosure of "secret," "criminal history" or "sensitive" information, except as permitted by law or regulation. Sec. 140-2.02(c)(3) permits dissemination of criminal justice information only to agencies and persons who need the information in the administration of criminal justice; however, investigative and intelligence data are not included among information categories that comprise "criminal justice information" according to Ga. Code § 35-3-30.

Hawaii
Hawaii Rev. Stat. §§ 92-50 to 92-52

Public records law exempts any records pertaining to a prosecution or defense prior to commencement of proceedings at the discretion of the attorney general or a responsible county attorney. It also exempts records unrelated to any violation of a law if disclosure would harm any person's reputation.

Idaho
Idaho Code § 9-301

Public records law contains no express exemption for I&I records but provides that any records may be exempt under other statutes.

Illinois
Ill. Stat. Ann. ch. 116, §§ 43.4 et seq. (Smith-Hurd)

Public records law exempts disclosures that would result in invasion of privacy. Criminal history records are exempt under ch. 38, § 210-1, except as necessary for identification.

Indiana
Ind. Stat. Ann. ch. 3, §§ 5-14-1-2, et seq. (Burns)

Sec. 5-14-3-4(1) exempts records declared "confidential" by statute. Intelligence records are declared confidential under ch. 4, § 5-2-4-6, which states that such information may be disseminated only to another criminal justice agency demonstrating a need to know.

Iowa
Iowa Code Ann. ch. 68A, §§ 68A.1 to 68A.9

Sec. 68A.7 exempts peace officers' investigative records except where disclosure is authorized elsewhere by statute. Intelligence data are categorized as nonpublic rec-

ords in ch. 692, § 692.18. Ch. 692, § 692.8 prohibits computer storage of intelligence data and permits dissemination of such information only to a peace officer, criminal justice or other agency if the department is satisfied that the need to know and intended use are reasonable.

Kansas
Kan. Stat. Ann. tit. 45, art. 2, § 45-201

Public records law contains no express exemption for I&I records but provides that any records may be exempt under other statutes. The dissemination of criminal history record information is restricted by tit. 22, art. 47, § 22-4707. I&I files are excluded from the definition of criminal history record information under tit. 22, art. 47, § 22-4701(b)(1).

Kentucky
Ky. Rev. Stat. ch. 61, §§ 61.870, et seq. (Baldwin)

Ch. 61, § 61.878(f) exempts investigative information before a related enforcement action is completed if disclosure would harm the agency by revealing the identity of an informant or by causing premature release of information to be used in an enforcement action. Ch. 17, §17.150(2) states that I&I records are open to inspection after prosecution is completed or a determination not to prosecute has been made; however, portions of such records may be withheld if: (A) disclosure would reveal the name of a confidential informant, (B) the information is personal and release would not advance a wholesome public interest, (C) release would endanger the life or safety of law enforcement personnel or (D) the information is to be used in a prospective enforcement action.

Louisiana
La. Rev. Stat. Ann. tit. 44, ch. 1, §§ 1 to 9

Tit. 44, ch. 1, § 3-A exempts all records of law enforcement agencies that: (A) pertain to criminal litigation until final adjudication, (B) contain the identity of a confidential source, (C) contain security procedures, investigative techniques, etc., (D) constitute arrest records until final judgment and (E) contain the identities of undercover agents. Sec. 3-B bars access to records tending to impart the identity of a confidential source. Under § 3-D, investigative records may be freely disseminated among law enforcement agencies.

Maine
Me. Rev. Stat. Ann. tit. 1, ch. 13, §§ 401 to 410

Public records law contains no express exemption for I&I records but provides that any records may be exempt under other statutes. However, tit. 16, subch. 8, § 614 contains an affirmative prohibition on the dissemination of I&I information that is triggered by the considerations embodied in the federal Freedom of Information Act. Such information shall not be disclosed if release may: (A) interfere with law enforcement proceedings, (B) result in public dissemination of prejudicial information concerning an accused person or concerning the prosecution's evidence that will interfere with the ability of the court to empanel an impartial jury, (C) result in public dissemination of information about the private life of an individual in which there is no legitimate public interest and which would be offensive to a reasonable person, (D) disclose the identity of a confidential source, (E) disclose confidential information furnished only by the confidential source, (F) disclose investigative techniques and procedures not generally known or (G) endanger the life or physical safety of law enforcement personnel. The information may be disseminated to other criminal justice agencies and the record subject with proper authorization.

Maryland
Md. Ann. Code of 1957 art. 76A

Art. 76A, § 3(i) substantively duplicates federal law, exempting I&I records to the extent that disclosure would: (A) interfere with valid and proper law enforcement proceedings, (B) deprive another person of a right to a fair trial or impartial adjudication, (C) constitute an unwarranted invasion of personal privacy, (D) disclose the identity of a confidential source, (E) disclose investigative techniques and procedures, (F) prejudice any investigation or (G) endanger the life or physical safety of any person.

Massachusetts
Mass. Gen. Laws Ann. ch. 66, § 10; ch. 4, § 7(f)

The term "public records" is defined to exclude "investigatory materials necessarily compiled out of the public view by law enforcement or other investigatory officials the disclosure of which materials would probably so prejudice the possibility of effective law enforcement that such disclosure would not be in the public interest." Ch. 4, § 7(f). Ch. 6, § 167 defines criminal offender record information as excluding I&I records. Under ch. 6, § 172, disssemination of criminal offender record information and "evaluative" information is limited to criminal justice agencies and other agencies and individuals under certain circumstances.

Michigan
Mich. Stat. Ann. § 4.1801

Sec. 4.1801(13)(1)(b) substantively duplicates federal law, exempting investigative records to the extent that disclosure would: (A) interfere with law enforcement proceedings, (B) deprive a person of the right to a fair trial or impartial adjudication, (C) constitute an unwarranted invasion of personal privacy, (D) disclose the identity of a confidential source or confidential information furnished only by a confidential source, (E) disclose law enforcement investigative techniques or procedures or (F) endanger the life or physical safety of law enforcement personnel.

Minnesota
Minn. Stat. Ann., ch. 13, §§ 13.01 to 13.87

Active investigative information is exempt. Ch. 13, § 13.82(5). Inactive investigative information is exempt under § 13.82(5) if release would jeopardize the identity of an undercover agent, informant, sex crime victim or any other victim or witness who has asked for confidentiality.

Mississippi
Miss. Code Ann. § 25-53-53 (1972)

Public records law contains no express exemption for I&I records but exempts all confidential data.

Missouri
Mo. Ann. Stat. § 109.180 (Vernon)

Public records law contains no express exemption for I&I records but provides that any records may be exempt under other statutes. Certain arrest records must be closed and withheld from disclosure under §§ 610.100 to 610.120.

Montana
Mont. Code Ann. tit. 2, ch. 6, §§ 2-6-101 to 102

Public records law provides that all records ar eprivate and not subject to disclosure requirements unless they are included among enumerated categories of "public writings." Tit. 44, ch. 5, § 44-5-103 defines "confidential" criminal justice information as including I&I records. Under § 44-5-303, dissemination of such information is restricted to criminal justice agencies or others authorized by law.

Nebraska
Neb. Rev. Stat. § 84-712

Investigative records are exempt under § 84-712.05(5) and may be withheld.

Nevada
Nev. Rev. Stat. ch. 239, § 239.010

Public records law exempts records declared by law to be confidential.

New Hampshire
N.H. Rev. Stat. Ann. §§ 91-A:4 and 91-A:5

Public records law contains no express exemption for I&I records but provides that any records may be exempt under other statutes. Sec. 91-A:5 exempts "confidential" data and information the release of which would constitute an invasion of privacy.

New Jersey
N.J. Stat. Ann. § 47:1A-1 to 1A-4

Records pertaining to an ongoing investigation may be withheld if disclosure would be inimical to the public interest under § 47:1A-3. Sec. 53:6-18 says that records of a bureau designated to maintain intelligence information may be made available only to police department officers and employees.

New Mexico
N.M. Stat. Ann. ch. 14, art. 2, §§ 14-2-1 to 14-2-3

Public records law contains no express exemption for I&I records but provides that any records may be exempt under other statutes.

New York
N.Y. Pub. Off. Law art. 6, § 87(2)(e)

Art. 6, § 87(2)(e) exempts all records compiled for law enforcement purposes if disclosure would: (A) interfere with law enforcement investigations or judicial proceedings, (B) deprive a person of a right to a fair trial or impartial adjudication, (C) identify a confidential source or disclose confidential information or (D) reveal criminal investigative techniques or procedures that are not routine. In addition, any information is exempt under § 87(2)(f) if disclosure would endanger the life of any person.

North Carolina
N.C. Gen. Stat. ch. 132, §§ 132-1 to 132-9

Public records law contains no express exemption for I&I records.

North Dakota
N.D. Cent. Code § 44-04-18

Public records law contains no express exemption for I&I records but provides that any records may be exempt under other statutes.

Ohio
Ohio Rev. Code Ann. 149.43 to 149.99 (Page)

Public records law contains no express exemption for I&I records but provides that any records may be exempt under other statutes.

Oklahoma
Okla. Stat. Ann. tit. 51, ch. 1, § 24

Public records law contains no express exemption for I&I records but exempts any records "required by law to be

kept secret." Under tit. 47, § 2-129, department of public safety employees charged with the custody of "confidential and privileged" information shall not disclose this information except to law enforcement agencies.

Oregon
Or. Rev. Stat. §§ 192.410 to 192.500

Sec. 192.500(1)(c) exempts investigative information compiled for criminal law purposes. However, arrest and crime report records shall not be confidential unless there is a clear need to delay disclosure in the course of an investigation.

Pennsylvania
Pa. Stat. Ann. tit. 65, ch. 3, §§ 66.1 to 66.4

Sec. 66.1(2) exempts any report, communication or other paper that would disclose the progress or result of an agency investigation as well as documents that would impair a person's reputation or personal security.

Puerto Rico
P.R. Laws Ann. tit. 32 § 1781

Public records law contain no express exemption for I&I records. The right of inspection of records generally does not extend to notes, memoranda or correspondence of government officials, nor to any information of a confidential nature that would create prejudice to the administration of the agency. 1966 Op. Sec. Jus. No. 46.

Rhode Island
R.I. Gen. Laws, tit. 38, ch. 2, §§ 38-2-1 to 38-2-12

Sec. 38-2-2(d)(4) exempts all records maintained by law enforcement agencies for criminal law enforcement, except records of an initial arrest and any complaint filed in court by a law enforcement agency.

South Carolina
S.C. Code Ann. tit. 30, ch. 4, §§ 30-4-10 to 30-4-110

Sec. 30-4-40(3) is similar to federal law and exempts investigative records if disclosure would cause harm by: (A) disclosing the identity of informants not otherwise known, (B) resulting in the premature release of information to be used in a prospective law enforcement action, (C) disclosing investigative techniques not otherwise known outside the government or (D) endangering the life, health or property of any person.

South Dakota
S.D. Codified Laws Ann. ch. 1-27, §§ 1-27-1 to 1-27-3

Public records law contains no express exemption for I&I records but Sec. 1-27-3 exempts records declared confidential or secret by law.

Tennessee
Tenn. Code Ann. §§ 10-7-503 to 10-7-509

Sec. 10-7-504(a) exempts all investigative records of the Tennessee Bureau of Criminal Identification. Sec. 10-7-504(c) exempts certain records of the attorney general's office, including those related to federal investigations that are confidential or privileged under federal law.

Texas
Tex. Rev. Civ. Stat. Ann., art. 6252-17a, §§ 1 to 15

Art. 6252-17a, §3(8) exempts all investigative records of law enforcement agencies and notations maintained for internal use in matters related to law enforcement. Sec. 3(1) exempts information deemed confidential by statute or case law and Sec. 3(3) exempts information relating to litigation of a criminal or civil nature.

Utah
Utah Code Ann. §§ 78-26-1 to 78-26-3

Public records law contains no express exemption for I&I records but provides that any records may be exempt under other statutes. Investigative records are exempt from the Archives and Records Service and Information Practices Act, which creates a central record management program. § 63-2-89.

Vermont
Vt. Stat. Ann. tit. 1, ch. 5, subch. 3, §§ 313 to 320

Sec. 317(b)(5) exempts investigative records.

Virginia
Va. Code ch. 21, §§ 2.1-340 to 2.1-346.1

Sec. 2.1-342(b)(1) exempts memoranda, correspondence, evidence and complaints related to criminal investigations as well as reports submitted to the police in confidence.

Virgin Islands
V.I. Code Ann. tit. 3, ch. 33, § 881

Sec. 881(g)5 mandates that peace officers' investigative reports be kept confidential except where disclosure is authorized by other statutes.

Washington
Wash. Rev. Code Ann. ch. 41.17, §§ 250 to 340

Ch. 42.17, § 310(1)(d) exempts "specific" I&I records where nondisclosure is "essential to effective law enforcement or for the protection of any person's right to privacy."

West Virginia
W.Va. Code ch. 29B, art. 1, §§ 29B-1-1 to 29B-1-6

Sec. 29B-1-4(4) exempts investigative records and internal notations of law enforcement agencies.

Wisconsin
Wis. Stat. Ann. § 19.31 to 19.39 (West)

Public records law exempts any law enforcement records that must be withheld from disclosure to qualify for federal funds and provides that any records may be exempt under other statutes.

Wyoming
Wyo. Stat. §§ 16-4-201 to 16-4-204 (formerly §§ 9-9-101 to 9-9-105)

Public records law contains no express exemption for I&I records but provides that any records may be exempt under other statutes. Sec. 9-1-627(c) exempts identification and intelligence information, making such information available only to law enforcement agencies.

APPENDIX B

TABLE OF CITATIONS

TABLE OF CITATIONS

Miscellaneous Publications

	Page
121 Cong. Rec., 11554 (April 23, 1975)	37
Criminal Justice Information Policy: Privacy and the Private Employer, Department of Justice (1981)	92
Davis, "Police Surveillance of Political Dissidents." Columbia Human Rights Law Review 4:101 (1972)	20,41
Dintino and Martens, Police Intelligence Systems in Crime Control, Thomas (1983)	9
1983 Domestic Security Guidelines, Sec. III.B.1.	37
Donner, The Age of Surveillance, Vintage (1981)	15,17
Draper, "Privacy and Police Intelligence Data Banks: A Proposal to Create a State Organized Crime Intelligence System and to Regulate the Use of Criminal Intelligence Information." Harvard Journal of Legislation 14:1 (1976)	16,19,20, 26,29,31, 35,37, 58,92
"The Erosion of Law Enforcement Intelligence and its Impact on Public Security," Before the Subcommittee on Criminal Laws and Procedures of the Senate Committee on the Judiciary, 95th Cong., 2d Sess. (1984)	22
FBI Guidelines for Domestic Security Investigations, published by Attorney General Levi on March 10, 1976	22
Federal Information Disclosure, pp. 17-20	67

	Page
Federal Information Disclosure, § 17.07	47,48
Federal Information Disclosure, § 17.04	48
Gilbert, Criminal Investigation, Charles Merrill Co. (1980)	9,13,14, 15,16,17, 18,26, 27,28
Godfrey and Harris, Basic Elements of Intelligence, LEAA (1971)	9,28, 29,35
Hatch, "Too Much Freedom Under FOIA," Am. Bar. Assoc. J., May 1983	73,74
"Hearings on Criminal Justice Data Banks" before the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary, 93rd Cong., 2d Sess. (1974)	21
"Hearings on Federal Data Banks, Computers and the Bill of Rights" before the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary, 92nd Cong., 1st Sess. (1971)	21
"Hearings on Military Surveillance" before the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary, 93rd Cong., 2d Sess. (1974)	21
"Hearings on Surveillance Technology: Policy and Implications, "Report of the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary, 94th Cong., 2d Sess. (1976)	21

NCJ-95787, 2/85
Intelligence & Investigative Records: Criminal Justice Information Policy

NCJRS REGISTRATION

The National Criminal Justice Reference Service (NCJRS) abstracts documents published in the criminal justice field. Persons who are registered with the Reference Service receive announcements of documents in their stated fields of interest and order forms for free copies of Bureau of Justice Statistics publications. If you are not registered with the Reference Service, and wish to be, please provide your name and mailing address below and check the appropriate box.

Name	Telephone ( )	☐ Please send me a NCJRS registration form.
Number and street		☐ Please send me the reports listed below.
City	State ZIP Code	

(Fold here)

U.S. DEPARTMENT OF JUSTICE
Bureau of Justice Statistics
Washington, D.C. 20531

PLACE STAMP HERE

User Services Department 2
National Criminal Justice Reference Service
Bureau of Justice Statistics
U.S. Department of Justice
Box 6000
Rockville, Maryland 20850

(Fold here)

If you wish to be put on the Bureau of Justice Statistics mailing list(s) or receive copies of recent BJS reports, please check them on the other side of this sheet and mail it in.

Bureau of Justice Statistics reports

(revised February 1985)

Call toll-free 800-732-3277 (local 251-5500) to order BJS reports, to be added to one of the BJS mailing lists, or to speak to a reference specialist in statistics at the Justice Statistics Clearinghouse, National Criminal Justice Reference Service, Box 6000, Rockville, MD 20850. Single copies of reports are free; use NCJ number to order. Postage and handling are charged for bulk orders of single reports. For single copies of multiple titles, up to 10 titles are free; 11-40 titles $10; more than 40, $20; libraries call for special rates.

Public-use tapes of BJS data sets and other criminal justice data are available from the Criminal Justice Archive and Information Network, P.O. Box 1248, Ann Arbor, MI 48106 (313-764-5199).

National Crime Survey

Criminal victimization in the U.S.:
- **1982** (final report), NCJ-92820, 11/84
- **1973-82** trends, NCJ-90541, 9/83
- **1981** (final report), NCJ-90208
- **1980** (final report), NCJ-84015, 4/83
- **1979** (final report), NCJ-76710, 12/81

BJS special reports:
- **The economic cost of crime to victims,** NCJ-93450, 4/84
- **Family violence,** NCJ-93449, 4/84

BJS bulletins:
- **Household burglary,** NCJ-96021, 1/85
- **Criminal victimization 1983,** NCJ-93869, 6/84
- **Households touched by crime,** 1983, NCJ-93658, 5/84
- **Violent crime by strangers,** NCJ-80829, 4/82
- **Crime and elderly,** NCJ-79614, 1/82
- **Measuring crime,** NCJ-75710, 2/81

Victimization and fear of crime: World perspectives, NCJ-93872, 1/85
The National Crime Survey: Working papers,
- vol. I: Current and historical perspectives, NCJ-75374, 8/82
- vol. II: Methological studies, NCJ-90307, 12/84

Crime against the elderly in 26 cities, NCJ-76706, 1/82
The Hispanic victim, NCJ-69261, 11/81
Issues in the measurement of crime, NCJ-74682, 10/81
Criminal victimization of California residents, 1974-77, NCJ-70944, 6/81
Restitution to victims of personal and household crimes, NCJ-72770, 5/81
Criminal victimization of New York State residents, 1974-77, NCJ-66481, 9/80
The cost of negligence: Losses from preventable household burglaries, NCJ-53527, 12/79
Rape victimization in 26 American cities, NCJ-55878, 8/79
Criminal victimization in urban schools, NCJ-56396, 8/79
Crime against persons in urban, suburban, and rural areas, NCJ-53551, 7/79
An introduction to the National Crime Survey, NCJ-43732, 4/78
Local victim surveys: A review of the issues, NCJ-39973, 8/77

Privacy and security

Computer crime:
- **Electronic fund transfer and crime,** NCJ-92650, 2/84
- **Computer security techniques,** NCJ-84049, 9/82
- **Electronic fund transfer systems and crime,** NCJ-83736, 9/82
- **Legislative resource manual,** NCJ-78890, 9/81
- **Expert witness manual,** NCJ-77927, 9/81
- **Criminal justice resource manual,** NCJ-61550, 12/79

Privacy and security of criminal history information:
- **A guide to research and statistical use,** NCJ-69790, 5/81
- **A guide to dissemination,** NCJ-40000, 1/79
- **Compendium of State legislation:** NCJ-48981, 7/78
  - **1981 supplement,** NCJ-79652, 3/82

Criminal justice information policy:
- **Victim/witness legislation: An overview,** NCJ-94263, 12/84
- **Information policy and crime control strategies** (SEARCH/BJS conference), NCJ-93926, 10/84
- **Research access to criminal justice data,** NCJ-84154, 2/83
- **Privacy and juvenile justice records,** NCJ-84152, 1/83
- **Survey of State laws** (BJS bulletin), NCJ-80836, 6/82
- **Privacy and the private employer,** NCJ-79651, 11/81

Federal offenses and offenders

BJS special reports:
- **Pretrial release and misconduct,** NCJ-96132, 1/85

BJS bulletins:
- **Bank robbery,** NCJ-94630, 8/84
- **Federal drug law violators,** NCJ-92692, 2/84
- **Federal justice statistics,** NCJ-80814, 3/82

General

BJS bulletins:
- **Tracking offenders: The child victim,** NCJ-95785, 12/84
- **The severity of crime,** NCJ-92326, 1/84
- **The American response to crime: An overview of criminal justice systems,** NCJ-91936, 12/83
- **Tracking offenders,** NCJ-91572, 11/83
- **Victim and witness assistance: New State laws and the system's response,** NCJ-87934, 5/83

BJS telephone contacts, NCJ-95505, 10/84
How to gain access to BJS data (brochure), BC-000022, 9/84
Sourcebook of Criminal Justice Statistics, 1983, NCJ-91534, 10/84
Information policy and crime control strategies, NCJ-93926, 10/84
Proceedings of the 2nd workshop on law and justice statistics, 1984, NCJ-93310, 8/84
Report to the nation on crime and justice: The data, NCJ-87068, 10/83
Dictionary of criminal justice data terminology: 2nd ed., NCJ-76939, 2/82
Technical standards for machine-readable data

END