APPENDIX E

Computerized Criminal Information and Intelligence Systems*

The application of computer technology to criminal justice information systems was recommended by the President's Crime Commission[1] as an important tool for improving the deployment of criminal justice resources and for keeping track of criminal offenders. The commission warned, however, that special precautionary steps would have to be taken to protect individual rights and recommended that primary control of computerized information systems be retained at the state and local levels to avoid the development of a centralized file subject to Executive manipulation.

LEAA [Law Enforcement Assistance Administration, Department of Justice] has effectively concentrated a variety of resources, including research, discretionary and block grants, in the development of computerized information and intelligence systems. It has not, however, given adequate attention to the warnings of the Crime Commission or demonstrated adequate appreciation of the consequences of a massive accumulation of personal dossiers at the national level.

Millions of dollars of [National] Institute [of Law Enforcement and Criminal Justice] and discretionary grants have supported the creation of a national computerized file of criminal histories that is fed by LEAA block grant-funded state information systems. The initial design of the system followed the decentralized model recommended by the Crime Commission, but in January 1970, former Attorney General John N. Mitchell decided—over the objections of LEAA—to make the system a more centralized one. To accomplish this purpose, he transferred the file system from LEAA to the FBI.

LEAA has simultaneously given the states substantial grants to create intelligence systems directed primarily toward organized crime, civil disorders and the activities of dissenters. . . . Some of these files are being maintained by the same agencies that operate the more reliable information files, creating the possibility that the two will be used jointly. At the federal level the Attorney General has the power to combine intelligence with information files, but he apparently has not exercised that power, on a regular basis.

All of this has occurred without broad public policy debate about the desirability of the new systems and with little serious effort to determine whether the contribution they make to controlling crime outweighs their potential for eroding privacy and individual autonomy, or whether that potential can be reduced or controlled.

LEAA's investment in information and intelligence systems must be placed in the context of the over-all Justice Department strategy for strengthening the law enforcement capability of the federal government and for building up the powers of police and prosecutors at all levels. During his tenure as Attorney General (1968-72) John N. Mitchell made it clear that these were major goals of his administration. To this end he greatly expanded federal surveillance of citizens thought to be threats to internal security, justifying his action on the theory that the Executive has inherent and discretion-

*Reprinted, with permission, from *Law and Disorder III: State and Federal Performance Under Title I of the Omnibus Crime Control and Safe Streets Act of 1968*, prepared under the direction of Sarah C. Carey for the Lawyer's Committee for Civil Rights Under Law (Washington, D.C.), 1973, Chapter II, pp. 41-49. The Acting Director of the FBI submitted comments on this paper for the record of *Hearings on Nomination of Louis Patrick Gray III*, before the Committee on the Judiciary, United States Senate, 93rd Cong., 1st Session (1973); the comments will be found at pp. 265-268 of the *Hearings*.

[1] The President's Commission on Law Enforcement and Administration of Justice. The Commission's report entitled, *The Challenge of Crime in a Free Society*, was published in February 1967.

ary power to protect itself.[2] He made aggressive use of existing laws, and sought and obtained significant new legislation to arm police and prosecutors with expanded authority to monitor individual conduct in order to prevent or punish potential crimes.[3] These developments, when viewed in conjunction with the new surveillance technology funded by LEAA grants and the national computerized file on criminal offenders, greatly increase the capability of the government to monitor the activities of all citizens and to step in to prevent or punish those activities where it chooses to do so.[4]

The new criminal justice information network can be used in conjunction with the vast government and private computer dossiers being compiled by credit bureaus, insurance companies, welfare agencies, mental health units and others.[5] Cumulatively, these files threaten an "information tyranny" that could lock each

[2] See the statement of William H. Rehnquist, *Hearings on Federal Data Banks, Computers and the Bill of Rights*, Senate Subcommittee on Constitutional Rights, 92nd Congress, 1st Session (February-March 1971) p. 597, *et seq.*, March 11, 1971. (Referred to hereafter as *Senate Constitutional Rights Subcommittee Hearings.*) The Supreme Court rejected the argument that warrantless wiretapping is permissible, in *United States* v. *United States District Court*, 407 U.S. 297, 40 U.S.L.W. 4761 (1972)

[3] For example, under Mitchell's leadership the Justice Department implemented Titles II (expanding federal wiretapping powers) and III (weakening the strict exclusionary rules developed after the Supreme Court's ruling in *Miranda* v. *Arizona*) of the Safe Streets Act of 1968. In addition the department has sought and obtained new legislation such as the D.C. Crime Bill, the Organized Crime Act of 1970 and the Comprehensive Drug Abuse Prevention and Control Act of 1970, which greatly expanded federal law enforcement powers. These three bills include a number of provisions of dubious constitutionality, such as authority for preventive detention of suspects, for police to enter homes without warning ("no-knock"), for courts to impose greatly expanded sentences for "dangerous special offenders," and for grand juries to function with increased powers.

[4] A recent federal court ruling on another matter describes the congressional intent *not* to create a national police force through the LEAA program. In *Ely* v. *Velde*, 451 F.2d 1131, at 1136 (4th Cir. 1972), the court stated: "The dominant concern of Congress apparently was to guard against any tendency toward federalization of local police and law enforcement agencies." Congress feared that "overbroad federal control of state law enforcement could result in the creation of an Orwellian 'federal police force'. . . .The legislative history reflects the congressional purpose to shield the routine operation of local police forces from ongoing control by LEAA–a control which conceivably could turn the local police into an arm of the federal government."

[5] The courts can and do protect individual's constitutional rights when they are specifically threatened by overt government action. But judicial intervention is, by nature, episodic and primarily remedial rather than preventive. Until governmental overreaching ripens into concrete, demonstrable injury–such as the use of illegal evidence at trial, the

citizen into his past; they signal the end of a uniquely American promise–that the individual can shed past mistakes and entanglements, and start out anew.

There are no federal and few state laws regulating the national criminal information system or its components. Few laws control the host of related public and private information systems. And any constitutional protections that exist are limited and narrowly defined.[6] Without controls, the systems continue to evolve primarily by force of their own momentum. In part through the well-meaning actions of LEAA the prophecy of Dr. Jerome Weisner, MIT president, is being realized:

> Such a depersonalizing state of affairs could occur without overt decisions, without high-level encouragement or support and totally independent of malicious intent. The great danger is that we could become information bound, because each step in the development of an information tyranny appeared to be constructive and useful.[7]

Computerized Criminal History Files

> When the LEAA program began [in 1969], a few states had established centralized files of criminal offender histories to assist police departments in the identification and prosecution of suspects. For example, New York State's Identification and Intelligence System (NYSIIS), operating on an annual budget in excess of $5 million, had more than two or three million fingerprints and 500,000 summary criminal histories on its computer.[8] Additional

(Continued)
loss of employment or the disbanding of a political organization–the courts will not recognize that it is harmful. See, for example, *Laird* v. *Tatum*, 408 U.S. 1, 40 U.S.L.W. 4850 (June 26, 1972), rejecting a claim that military surveillance of persons involved in domestic political activities violates the Constitution.

[6] In many ways these data banks are far more threatening than those maintained by criminal justice agencies. The over-all problem of computers and privacy is well presented in Miller, *Assault on Privacy: Computers, Data Banks and Dossiers* (1972), and in the hearings cited above, n.2.

[7] *Senate Constitutional Rights Subcommittee Hearings*, March 11, 1971, p. 671.

[8] NYSIIS performs a variety of functions in regard to this data: fingerprint processing (not yet computerized), name searching, wanted system (NCIC interface), personal appearance/arrestee file searches and review of latent fingerprinting material.(NYSIIS Fact Sheet)

fingerprints and criminal histories existed in manual files. Included in both the files were "criminal wanteds" for felonies and misdemeanors, escapees from penal institutions, parole and probation absconders, elopees from mental institutions and missing persons. More than 3,600 local law enforcement agencies submitted information to the files and used them to check out suspects and new arrests. Other states, such as California, Michigan and Florida, were developing systems, but for the most part centralized, computerized record-keeping was rudimentary. The extent to which the state files expedited or otherwise improved law enforcement had not been demonstrated.

At the national level the FBI maintained the National Crime Information Center (NCIC). This system operated through local law enforcement control terminals (as of early 1972 there were 102 terminals, of which 48 were computerized) that put the FBI in direct touch with approximately 4,000 of the nation's 40,000 local law enforcement agencies. NCIC cost about $2.3 million per year to operate. The system contained files on stolen items, such as vehicles, firearms, boats and securities, and on wanted persons. Of the 3.1 million NCIC files, only about 300,000 were active criminal offender records. On an average, the NCIC system found a record or produced a "hit" on about 6 percent of the queries it received from local agencies (some estimates have been as low as 2 percent). In addition to the NCIC system, the FBI maintained more than 190 million identification and fingerprint files and approximately 20 million criminal offender records in permanent manual files.

Federal, state and local law enforcement agencies all contributed information to and could extract information from the NCIC files. In addition, NCIC records were searched as part of the identification service that the FBI provides for agencies of federal and state governments and other authorized institutions, including hospitals and national banks, which seek information on an individual's arrest record for purposes of employment clearances and licensing.[9]

[9] Executive Order 10450 (April 1953) calls for an investigation of any individual appointed "in any department or agency of the government," and provides that "in no event shall the investigation include less than a national agency check (including a check of the fingerprint files of the FBI), and written inquiries to appropriate local law enforcement agencies. . . ." In *Menard* v. *Mitchell*, 328 F. Supp. 718 (D.D.C. 1971), the court suggested the Executive Order should be reexamined, but refused to enjoin the use of NCIC for this purpose. The court did preclude the distribution of arrest records except for law enforcement and federal employment purposes, but Congress overruled this exclusion in approving the FBI's 1972 appropriation (See n. 29, *infra*)

Today it is clear the NCIC and the few systems such as NYSIIS were relatively primitive, first generation data banks. In the past three years, with the investment of more than $50 million in Institute, discretionary and block grant funds, LEAA has launched a program that by 1975 promises computerized criminal history files kept by all 50 states that will be tied in to ("interfaced with") a massive national file run by the FBI. The states will place in the central FBI file only information of public record pertaining to people who have been accused of "serious and other significant violations." The central file will consist of comprehensive histories of persons who violate federal laws or who commit crimes in more than one state and summary histories on offenders who have been involved solely in intrastate crimes.[10] Any authorized inquirers[11] will have access to the central records, and will be referred to the relevant state files for further information. The individual state systems will include whatever information or intelligence the states choose to put into them and will be accessible on terms defined by each state.

This ambitious centralized program developed out of the System for Electronic Analysis and Retrieval of Criminal Histories (Project SEARCH), a $16-million demonstration project supported by LEAA discretionary and Institute grants, in which 20 states shared criminal histories through a computerized central data index.[12] SEARCH was intended as a prototype for a national computer file which would facilitate prompt apprehension of interstate felons.[13]

[10] Summary criminal histories contain public record information such as fingerprints (where available), personal description, arrests, charges, dates and places of arrest, arresting agencies, court dispositions, sentences, limited institutional data and limited information concerning parole and probation.

[11] "Authorized inquirers" include any agency that now participates in the FBI's system, plus any agency subsequently permitted to do so by the Attorney General.

[12] The states participating in the SEARCH experiment were Arkansas, Arizona, California, Colorado, Connecticut, Florida, Georgia, Illinois, Maryland, Massachusetts, Michigan, Minnesota, Nebraska, New Jersey, New York, Ohio, Pennsylvania, Texas, Utah and Washington.

[13] As the FBI put it: "The purpose of centralization. . .is to contend with increasing criminal mobility. (NCIC Advisory Board, "Computerized History Program: Background,

(Continued)

The project was funded through the California Council on Criminal Justice. Primary developmental responsibility was contracted to Public Systems Inc. (PSI), a research and development firm based in San Jose.[14] PSI was aided by task forces and advisory committees composed of representatives from the participating states. The major assignment of the SEARCH group was to develop standard, computerized criminal history records, summaries of which could be filed in a central index. Computer terminals in the individual states could submit information to the central index and query it for identification of suspects. If the central index contained matching references concerning the subject of a query, the summary index data was transmitted to the inquiring police officer and he was told which state had the full file on the suspect. The officer could then request and obtain a copy of the suspect's full record via teletype from the state agency. The initial focus of the system—like its predecessors—was on police requirements; but the project design anticipated subsequent development of a capability to service the information needs of courts and corrections officials as well.[15]

On March 9, 1971, LEAA Associate Administrator Richard W. Velde testified before the Senate Subcommittee on Constitutional Rights that:

> The basic problems facing SEARCH in the demonstration period have been solved. A common format for criminal histories was developed, and in machine-readable form. Each active participant converted at least 10,000 felony records to the SEARCH system for the demonstration. As the test period showed, a state making an inquiry of the central index with perhaps no more information than a driver's license number could find out if that person were in the (national) index and then be switched to the state holding the complete criminal history. It takes merely seconds to do all of that and receive the information.[16]

Computer experts were less sanguine about the success of the experiment. Some noted that only a small number of the SEARCH states had actually participated in the demonstration and suggested that the test simply duplicated what the FBI's NCIC had already demonstrated. *Datamation* magazine reported on the SEARCH demonstation as follows:

> Ten states officially participated in the demonstration, but only New York made any extensive operational uses of the system, and a total of only five states conducted any demonstrations. . . .SEARCH met its demonstration objectives from a conceptual point of view, but did not achieve much operational success, because of design compromises, lack of updating capability for the central index and failure to develop record formats acceptable to all users, among other reasons.[17]

Despite these criticisms, and over the protests of LEAA Director Jerris Leonard and the states that had participated in the project, SEARCH became the launching pad for an expanded and "improved" criminal offender system to be operated by the FBI. Transfer of system control to the FBI meant that, instead of a network of state-controlled files tied into a limited central index, the SEARCH system became a national file run by a line operating agency. More importantly, judging from the debate on the subject that raged for months, FBI control meant diminished operational standards for the system's integrity, and attenuation of safeguards for individual privacy.

(Continued)
Concept and Policy," as approved March 31, 1971, and amended Aug. 31, 1971.) FBI data show that 25 percent of arrests involve interstate movement by felons. A preliminary survey by SEARCH put the figure at around 27 percent but estimated that most of these arrests were in contiguous states.

[14] Eight of PSI's key personnel are from Sylvania Sociosystems Lab (a research and development arm of GTE Sylvania), and one is the former head of California's SPA, the California Council on Criminal Justice.

[15] We disagree with LEAA's assumption that across-the-board increases in offender data are desirable for all decision-making processes within the criminal justice system. For example, arrest records not followed by convictions or juvenile offenses probably should not be made available to sentencing judges or to parole boards. LEAA recently made a grant to the Federal Judicial Center to finance the transfer of all data processed through the Federal courts to the Justice Department. Sen. Ervin has questioned the propriety of this arrangement under the separation of powers principle. (Letter of July 27, 1972, from Sen. Ervin to the Hon. Alfred P. Murrah, Federal Judicial Center.)

[16] *Senate Constitutional Rights Subcommittee Hearings*, p. 611.

[17] Phil Hirsch, *Datamation* magazine, June 15, 1971, pp. 28-31.

The conflict between the FBI and the Project SEARCH group had emerged in May 1970. In a letter dated May 8, 1970, Jerome J. Daunt, then director of the FBI's NCIC system, wrote to the SEARCH group complaining about various recommendations in the Interim Report of the SEARCH Committee on Security and Privacy. Among other items, the letter stated:

> Throughout the report Project SEARCH is described as an ongoing system. Future developments of this system are not the proper objectives of the Project SEARCH group. . . .
>
> In view of the limited purpose of the Project SEARCH, further studies in the area of privacy and security are not jusitified. If there is a need, it should be done by some other body.

The conflict became more pointed. In a letter of Oct. 15, 1970, John F.X. Irving, then chairman of the state planning agency's executive committee, wrote to Attorney General Mitchell protesting the proposed transfer of control over the SEARCH system to the FBI as well as certain "changes in direction" of the system. Irving complained that duplication would result because the states intended to continue developing their own systems[18] and protested that the FBI's plan to focus on data useful to the police only ignored the needs of courts and corrections agencies. Irving also argued that the FBI system, by dealing directly with city police departments instead of going through the states, would subvert the federal-state relationship contemplated by the Safe Streets Act.

The strongest protest in Irving's letter was directed to the potential invasions of privacy inherent in a federal information system.

> Last, but certainly not least, the FBI's proposed file is significantly different in both conception and content from the state-held files contemplated by Project SEARCH. The basic underlying concept of Project SEARCH is that no new national data banks or criminal history files should be created because of the inherent threats to individual privacy and the security of records. The Project SEARCH operating concept is state-held files with a national index or directory of offenders. . . .The FBI file, on the other hand, would contain as much detailed data on offenders as the FBI was willing and able to collect. It is not a true index but rather a federal data bank on offenders.

[18] By altering the basic system design for SEARCH, FBI requirements could increase the cost by 30 to 40 percent, apart from the possible duplication involved. Interview with Jerry Emmer, LEAA official.

The FBI countered that expanding SEARCH as a state-dominated system would increase the over-all costs and would duplicate the NCIC system. More importantly, a system subject to the control of 50 state executives could be abused too easily. As Jerome Daunt put it: "If the governor controlled the system, he could control who gets elected."

The protests by the states and by Jerris Leonard were to no avail. The FBI took control of the SEARCH index in December 1970. The decision was John Mitchell's. In November 1971 the bureau notified the press that:

> The Federal of Investigation has begun operation of a computerized criminal history data bank that eventually will give police almost instantaneous access to an individual's criminal arrest record from all 50 states and some federal investigative agencies and the courts. . . .The system. . .will make available by 1975 on a nationwide computer network most of the information now handled through the FBI's vast criminal record and fingerprint files. . . .It replaces a pilot effort, called Project SEARCH, in which only a computerized index was maintained, capable of telling police if a suspect had a record.[19]

Although the November 1971 announcement signaled the end of LEAA control of the system, the agency has continued to be involved in the development and expansion of information systems. Project SEARCH has been given discretionary and research grants for developing related technology, such as satellite transmission of information, automatic fingerprint indentification/veritication and additional work on transaction-based criminal justice statistics. And

[19] Justice Department news release, November 1971.

LEAA block grants have continued to serve as the primary source of funding for the state information systems that will be the major components of the NCIC criminal history information system. Despite LEAA's expressed concern for privacy considerations in the operation of information systems, it has not sought to precondition the use of its funds for such systems on the development by the states of adequate statutory or regulatory safeguards.

It is difficult to obtain reliable information concerning the present or projected scope, cost or structure of the new FBI data bank. At the federal level a variety of agencies are scheduled to participate in the system, most of which have been previously active in the NCIC system. Among others, the system will receive data and answer inquiries from the Secret Service, the Internal Revenue Service, the Alcohol and Tax Division of the Treasury Department, the Bureau of Customs, the Immigration and Naturalization Service, the Bureau of Prisons, the U. S. Attorneys and U. S. Marshals. As far as the states are concerned, at the time of the FBI's November 1971 press release, only one state–Florida–was actually contributing information to the file. The next two states–New York and California–were not scheduled to participate until July 1972. (. . .California will probably not be ready for full participation until 1973.) In most instances, the states do not have their own systems operational–or even designed.

Official estimates of the total number of individuals who will eventually be included in the national file range from five million (the FBI estimate) to 20 million or more (the LEAA estimate). The number of files in the total system including all the state files will, of course, be much greater. Neither LEAA nor the FBI will provide information on the total costs involved.

Nor is it clear whether the FBI's file will be comprehensive, or simply a summary index that refers inquirers to the state files. The FBI has stated that it plans to maintain complete files only on offenders who have been arrested in more than one state, maintaining "summary files" on offenders who have been arrested within a single state only. State control centers will be able to add or remove information from the national file. However, for those states that have not yet built a central computerized information file, the FBI is presently maintaining complete offender files in both situations. The fact that the agency is presently maintaining

complete files for all states makes is doubtful that they will subsequently abandon those files.[20]

The kinds of information to be stored in the data file and the conditions of participation in the system are not defined by statute or by formal regulations. The only standards regulating the system are those set forth in the NCIC Advisory Board policy paper.[21] Each state seeking to participate in the system must sign a contract with the director of the FBI, agreeing to abide by the terms of the policy paper and by any "rules, policies and procedures hereinafter adopted by NCIC." The contracting state must also agree to indemnify the federal agency against any legal claims arising out of the operation of the information system. The FBI claims that the majority of the states–"all but three or four," according to Daunt, "and those have technical not substantive problems with the system"–have signed the contract and thereby accepted the terms of the policy paper.

The NCIC standards are substantially less rigorous than those developed by LEAA's Project SEARCH, and in many instances their adoption was met by vigorous objections from LEAA, the SPAs [state planning agencies] and the Project SEARCH participants.

Under the NCIC policies, the national file is restricted to data on "serious and other significant violations." This is defined by exclusion:

> Excluded from the national index will be juvenile offenders as defined by state law (unless the juvenile is tried in court as

[20] The basic policies developed for the FBI system by the NCIC Advisory Policy Board state:

> In the developed system, single state records will become an abbreviated criminal history record in the national index with switching capability for the states to obtain the detailed record. Such an abbreviated record should contain sufficient data to satisfy most inquiry needs, i.e., identification segment, originating agency, charge data, disposition of each criterion offense and current status. This will substantially reduce storage costs and eliminate additional duplication.

[21] The NCIC Policy Paper, *supra* n. 13. The board is appointed by and serves at the discretion of the director of the FBI. Its members are individuals responsible for the administration of state information systems or state or local terminals on the NCIC system. Recently, procedures were introducted for electing board members from among participating state officials. It does not include constitutional lawyers, computer experts or other nonlaw enforcement representatives.

an adult); charges of drunkeness and/or vagrancy; certain public order offenses, i.e., disturbing the peace, curfew violations, loitering, false fire alarm; traffic violations (except data will be stored on arrests for man-slaughter, driving under the influence of drugs or alcohol, and "hit and run"); and non-specific charges of suspicion or investigation.[22]

Narcotic or mental commitment records will be maintained if they are part of the criminal justice process. Domestic crimes such as nonsupport or adultery and victimless crimes such as homosexuality, gambling and others are considered "serious" in some jurisdictions.[23] Moreover, any state or locality may store additional information in its own files, which can be disseminated upon requests referred to the state or local police department by the central index.[24] Besides the criminal record data on serious offenders, the Justice Department has asserted an absolute right to keep records on persons who are "violence prone" and other "persons of interest" for national security reasons.

Contributions to each individual file depend on participating state and local agencies. According to the NCIC policy paper, each file is supposed to show arrests, charges, the disposition of each case, sentencing details and custody and supervision status, but experience indicates that agencies contributing to the files rarely remove arrests records that do not lead to convictions[25] and often

[22] NCIC Policy Paper, *supra* n. 18 p. 11.

[23] HR 1, the welfare reform proposal which was extensively revised by the Senate Finance Committee before the 92nd Congress adjourned, would make nonsupport a federal crime and place a special assistant U.S. attorney in every judicial district to prosecute violators whose desertion caused their families to go on welfare. This new crime would assure that personal data files on welfare recipients will be mingled with the files on criminal offenders.

[24] A number of jurisdictions maintain harmful, irrelevant data. The Kansas City, Mo., ALERT System, for example, includes the following categories of information in its computerized Warrant/Want Real Time Files: "local and national intelligence on parole status; active adult and juvenile arrest records with abstract data, area dignitaries; persons with a history of mental disturbance; persons known to have confronted or opposed law enforcement personnel in the performance of their duty; college students known to have participated in disturbances primarily on college campus areas." (Statement of Sen. Charles Mathias, March 9, 1971, *Senate Constitutional Rights Subcommittee Hearings*, p. 576.)

[25] The inclusion of arrest records that do not lead to conviction is particularly onerous. In 20 to 30 percent of arrests, the police do not bring charges for a variety of reasons

include damaging extenuating information. Personal identification information such as name, age, sex and physical description are included as well as FBI numbers, state numbers, social security numbers, date and place of birth and other miscellaneous numbers. At least one criminal fingerprint card is filed in the FBI identification division "to support the computerized criminal history record in the national index."[26]

No federal law or regulation calls for deletion of outdated records. The NCIC policy paper states: "Each control terminal agency shall follow the law or practice of the state. . .with respect to purging/expunging of data entered by that agency in the nationally stored data" (p. 12). Most states have no purging requirements at present. The policy paper endorses the concept of state and federal penalties for misuse of the data,[27] and suggests that the individual be given the right to see and correct his file, but makes no specific recommendations. Experience at the state and local levels indicates that it is extremely difficult for an individual to correct an erroneous or incomplete file without resorting to lengthy court proceedings.

The major deficiency in the guidelines and the system as a whole is the absence of proper controls on access to the data contained in the files. The policy paper states that access will be provided primarily to criminal justice agencies in the discharge of their official responsibilities. In addition, "agencies at all governmental levels which have as a principal function the collection and provision of fingerprint identification information" will have access, as will all those agencies that presently use NCIC. This means that the files will still be used for clearing Federal employees and the

including mistaken identification, lack of evidence, etc. Yet only eight states have statutes providing for expungement of such records. And of the eight, only one allows expungement of arrest records for an individual who has had a previous conviction.

[26] NCIC Policy Paper, *supra* n. 13.

[27] At present the only penalty for misuse of data maintained in the NCIC system is the provision in 28 USC §534 allowing the FBI to withdraw the privilege of participating in the exchange system from an agency that fails to abide by NCIC standards. As the exercise of that sanction means that the agency would also cease contributing data to NCIC, the provision has been invoked rarely. 18 USC §1905 provides weak criminal sanctions for the disclosure of confidential financial information by federal officials. It would not extend to the state participants in the NCIC system, and it protects only white-collar criminals whose offenses involve financial misdealings.

employees of Federal contractors,[28] and the information will be shared with federally insured banks, hospitals, insurance companies, etc.[29]

At the stage level, the NYSIIS experience suggests that a wide range of state agencies and some private firms will have access to the files for clearing potential employees or licensees.[30] The guidelines provide that state agencies (except for criminal justice agencies) cannot use the data in connection with licensing or state and local employment, unless "legislative action at the state and federal level or Attorney General Regulations" provide otherwise. But, as the New York experience shows, a number of states already have clearance authorization laws, and, since Congress has authorized the sharing of identification information with such states—with the approval of the Attorney General—the exclusion promises to be of limited value. (The Attorney General has never withheld approval from a state agency seeking access.) Even if approval or clearance should be denied, local policy will inevitably determine the terms of access because the NCIC system lacks adequate sanctions to apply to nonconforming states. At least one state, Iowa, is considering making the information available to anyone willing to pay for it.[31]

[28] Federal contractors such as Lockheed Aircraft have in the past obtained such records from the federal departments with which they do business.

[29] On Dec. 3, 1971, Congress approved, as part of the fiscal 1972 FBI appropriation, the following blanket authorization for the distribution of FBI data:

> The funds provided in the Department of Justice Appropriations Act, 1972 for Salaries and Expenses, Federal Bureau of Investigation, may be used, in addition to those uses authorized thereunder, for the exchange of identification records with officials of federally chartered or insured banking institutions to promote or maintain the security of those institutions, and, if authorized by state statute and approved by the Attorney General, to officials of state and local governments for purposes of employment and licensing, any such exchange to be made only for the official use of any such official and subject to the same restriction with respect to dissemination as that provided for under the aforementioned Act. (*Congressional Record*, Dec. 3, 1971, S 20461.)

In 1972 a proposal was submitted to Congress to reverse the 1971 action. At the time of this report that proposal, an amendment to the pending Justice Department appropriation bill, was before a House-Senate Conference Committee. In the meantime the Justice Department (through Sen. Hruska) introduced S 3834 (HR 15929) to assure the broad availability of FBI records.

[30] See letter from Aryeh Neier, executive director of the American Civil Liberties Union, to Sen. Sam J. Ervin (D-N.C.), March 23, 1971 (copy on file with the Senate Subcommittee on Constitutional Rights), listing state agencies with access to NYSIIS files.

[31] *Des Moines Sunday Register*, July 2, 1972, p. 3A.

The looseness of the access provisions becomes more ominous in view of the parallel rapid growth of law enforcement intelligence files containing sensitive and unsubstantiated information.[32] In addition, the provisions virtually invite linkages with information files maintained by public and private agencies. LEAA is presently cooperating with HUD and several other federal agencies to fund experimental programs in six cities[33] that will provide city managers or mayors with "integrated municipal information systems" (IMIS) for management purposes. The IMIS is being promoted by the National League of Cities as a "significantly new approach to the process of local government itself," one "that will require a degree of commitment and level of expenditure by municipalities which has never before been associated with computer-based systems." The new systems will eventually include data from all urban service departments—police, welfare, schools, etc.—as well as underlying demographic and other facts that could be useful in making urban management decisions. The enlarged, organized data base supposedly will point to new relationships among urban problems, and consequently will improve policy-making.

The IMIS could present serious problems;. . .As Robert Knisely, the director of the program, has written:

> If vital statistics, and school, employment and criminal justice records can be pulled together on a named individual at will, a child's teachers may find out he is illegitimate, his poor grades may keep him from getting a job, his lack of a job may

[32] We have already pointed out that LEAA is funding regional and state intelligence networks for the collection and analysis of data on organized crime, as well as state and local intelligence-gathering systems on civil disorders and militants and other nonconformers. Because of the difficulty of standardizing intelligence information, it is unlikely that interstate computer exchange of such data will be realized, at least for some time. However, once the data are centralized at the state level under the auspices of the agency responsible for operating the central criminal information files, it becomes accessible to other state or federal agencies who will be directed to the state of record through the NCIC system. And the Attorney General has the power under the present statutory scheme to combine federal investigative and intelligence files with the NCIC criminal offender files.

[33] The IMIS cities are: Dayton, St. Paul, Long Beach, Calif., Reading, Pa., Charlotte, N.C., and Wichita Falls, Tex. Other jurisdictions are combining criminal justice computer data with information from other public agencies on their own.

lead to crime and his criminal justice records may keep him permanently unemployed.[34]

Although Knisely sees certain potential benefits in the program, he concludes that they are overbalanced by the likelihood that neither the courts nor the legislatures will exert adequate control over the emerging technology. In any event, the possibility that criminal information files will become a part of a larger citywide integrated information system is a real one. In California, Iowa and other jurisdictions, data from a variety of social service agencies are already being combined in a single administrative unit that is also responsible for criminal justice data.[35]

Beyond IMIS, which is a deliberate, small-scale experiment, it is likely that private and public decision-makers will step up their generalized demands for whatever data are available on the individuals with whom they are concerned.[36] Senator Sam Ervin (D-N.C.) has described the problem this way:

> 'Interrelationship' is the key word here. Once the correlating process begins on individual personal data in the many files of government, all the weaknesses and limitations of the computer as a machine will be operating on a grand scale to make possible a massive invasion of the privacy of millions, and it raises the spectre of a possible program of routine denial of due process. Interagency, inter-business networks are being established of computers that talk only to each other . Decisions affecting a person's job, retirement benefits, security clearance, credit rating or many other rights may be made without benefit of a hearing or confrontation of the evidence.

[34] Knisely, Robert A., "The Fruit of the Tree of Knowledge–Privacy Problems in Integrated Municipal Information Systems," Dec. 7, 1971, p. 7.

[35] Iowa's TRACIS (Traffic Records and Criminal Justice Information System), for example, will connect with the state's Department of Public Instruction, the Department of Social Services and others. And the California CLETS system. . . .will be able to relate to records from the public schools.

[36] In recognition of this growing tendency and the immense data files available through his department, particularly those tied into social security numbers (as is the NCIC system), HEW Secretary Elliot L. Richardson has appointed an Advisory Committee on Automated Personal Data Systems to develop safeguards to "protect against potentially harmful consequences to privacy and due process." (See "Charter of the Secretary's Advisory Committee on Automated Personal Data Systems," Feb. 27, 1972.)

> The computer reduces his opportunity to talk back to the bureaucrats. It removes his chances to produce documents, photographs or other evidence to alter a decision.[37]

The problem of potential linkages between criminal justice systems and other governmental files on individuals has been centered in a debate that has plagued the new system since its inception. The NCIC guidelines initially required participating states to utilize computers "dedicated" to law enforcement uses only and managed by law enforcement personnel. Many of the states have opposed this policy on the grounds that dedicated computers cost more and, in some cases, that state law requires that all computer systems be centralized under the control of the governor.[38] According to Donald Roderick, Jerome Daunt's successor, the FBI will now permit each state to set its own rules in accordance with existing provisions for statewide computer administration. If a decision is reached to use a non-dedicated computer, however, that state must make a showing that the criminal justice data are under the control of law enforcement officials.

The Need for New Legislation

Neither the FBI nor LEAA, the two agencies of the Justice Department with the resources or powers to impose regulatory controls, has developed adequate safeguards for the fastgrowing computer files on criminal offenders. The NCIC guidelines are inadequate. As we have indicated, most of them are nonspecific, relying on state statutes to spell out specific protections. Since most of the states have no regulatory legislation on the books and the few laws that have been passed are inadequate, the system affords

[37] "The Computer and Individual Privacy," address of Sen. Sam J. Ervin (D-N.C.) to the American Management Association, March 6, 1967.

[38] Jerris Leonard sided with the states saying, "As long as I am here, we are going to carry out the philosophy of this administration and that is the states will decide what they need. . .If the FBI doesn't want to provide the service, we'll find someone else." (Washington *Evening Star*, Jan. 22, 1972). In addition the National Association for State Information Systems formally protested the dedication requirement to Attorney General Mitchell.

little protection against abuse. Further, the enforcement of the few NCIC standards that are binding depends exclusively on the FBI's willingness to exclude a noncomplying state from the system. This ultimate sanction has never been invoked.

Project SEARCH developed more comprehensive privacy and operational guidelines,[39] but these guidelines are advisory only, and not legally binding on the states. LEAA has been unwilling to impose the SEARCH standards as a condition of its grants. It has simply suggested that states contemplating the purchase of information systems with LEAA money "ensure that adequate provisions are made for system security, for protection of individual privacy and the insurance of the integrity and accuracy of the data collection."

Congress anticipated the need for regulation of the growing law enforcement information network in 1970 and added an amendment to the Safe Streets Act requiring LEAA to submit legislation by May 1, 1971, to ensure:

> The integrity and accuracy of criminal justice data collection, processing and dissemination systems funded in whole or in part by the federal government, and protecting the constitutional rights of all persons covered or affected by such systems.

On Sept. 20, 1971, Senator Roman Hruska (R-Neb.) introduced S 2546, "The Criminal Justice Information Systems Security and Privacy Act of 1971," on behalf of the Administration. The bill essentially would codify the standards established by the NCIC policy board and give the Attorney General the authority to alter the scope of the national system as he deems necessary. The bill, which has been severely criticized for failing to provide adequate protection against misuse of data, was never assigned to an appropriate subcommittee for hearings.

In addition in 1970 Congress mandated the creation of a National Commission on Individual Rights to study, among other things, the impact "of the accumulation by law or required by

[39] See Technical Report No. 2, July 1970, "Security and Privacy Considerations in Criminal History Information Systems," prepared by the Project SEARCH Committee Security and Privacy. The committee has also prepared a model state statute and model regulations for the governance of state information systems. These have been introduced but not acted upon in several state legislations.

executive action" and to determine which practices "are effective, and whether they infringe upon the individual rights of the people of the United States." (Title XII, The Organized Crime Control Act of 1970.) This provision has never been implemented.

There are serious questions whether the state and national computerized files are necessary, whether they are worth their cost, both social and financial, and whether they work. Perhaps with more experience the FBI or LEAA will develop a convincing case concerning the manner in which the computerized information systems have developed. However, the Justice Department has not yet confronted the very real problems that the new NCIC system is creating, particularly in regard to governmental overreaching, invasions of privacy and infringement of basic constitutional rights.

Underlying the deficiencies of the new NCIC criminal offender records system is the vagueness of the legislation under which it operates. 28 USC §534 enables the Attorney General to set up (and alter) a system to "acquire, collect, classify and preserve identification, criminal identification, crime and *other records.*" and to "exchange these records with, and for the official use of, authorized officials of the federal government, the states, cities and penal and *other institutions.*" (Emphasis added.) The statute contains no standards; and despite the fact that the Attorney General has full power to do so, no regulations have ever been issued to govern the information system except to delegate the Attorney General's administrative authority to the FBI (28 CFR § 0.85).

In addition to the question of the Justice Department's statutory power, several aspects of the system as it is presently administered raise important constitutional questions. To include information unrelated to criminal convictions in the state files (and by automatic referral in the national file) may well violate the First Amendment and the due process and equal protection clauses of the United States Constitution.

For example, on numerous occasions the Supreme Court has held or indicated that the Fifth and Fourteenth Amendments' guarantee of due process protects individuals from injury caused by public bodies acting without giving the individual the opportunity to challenge or clarify the factual assumptions on which the agency is

operating.[40] The protection against arbitrary action and the right to be heard apply even when the activities involved do not entail direct civil or criminal penalties, and extend to the circulation by the government of prejudicial information.

In *Joint Anti-Fascist Refugee Committee* v. *McGrath*,[41] the Supreme Court confronted a situation remarkedly similar to that posed by certain aspects of the present-day Justice Department data distribution program. Ruling that the Attorney General must provide an opportunity for a hearing before including an organization on his subversive list, Justice Felix Frankfurter stated:

> The heart of the matter is that democracy implies respect for the elementary rights of men, however suspect or unworthy; a democratic government must therefore practice fairness; and fairness can rarely be obtained by secret one-sided determination of facts decisive of rights. . . .No better instrument has been devised for arriving at truth than to give a person in jeopardy of serious loss notice of the case against him and opportunity to meet it. . . .The Attorney General is certainly not immune from the historic requirements of fairness merely because he acts, however conscientiously, in the name of security. 341 U.S. at 110-114.

Under the new NCIC system the federal and state agencies which disseminate background intelligence information or data pertaining to arrests not followed by conviction, without giving the subject the chance to clarify or correct his record, could be found in violation of the due process clauses of the Fifth and Fourteenth Amendments.

[40] See, e.g., *Joint Anti-Facist Refugee Committee* v. *McGrath*, 341 U.S. 123 (1951); *Greene* v. *McElroy*, 360 U.S. 474 (1959).

[41] *Supra*, n. 40. Although the Attorney General was ordered to institute proper procedures before adding an organization to the subversive list, the majority of the Court did not join any one opinion. Justice Frankfurter's constitutional reasoning has become the most noted of the opinions entered in that case. In *Winsconsin* v. *Constantineau*, 400 U.S. 433 (1971), the Supreme Court held unconstitutional a Wisconsin statute authorizing local authorities to post public notices prohibiting the sale of liquor to persons who drink excessively, without affording the interdicted individual a right to challenge the determination.

It is also quite possible that the NCIC criminal history file violates the equal protection clause, by magnifying the consequences of present discriminatory police practices. Because the data it collects focus on street crimes and offenses that tend to be committed by the disadvantaged and minorities, and because of its indiscriminate inclusion of data on arrests for ill-defined crimes (such as arrests for suspicion) and arrests not followed by charges or convictions, the NCIC file reinforces the existing class and racial bias of the criminal justice system. Arrests for "suspicion" or "investigation," for vagrancy and other vague crimes, constitute a major form of police discrimination against blacks and Chicanos. Keeping permanent computerized files of such arrests (and in some cases convictions) adds another layer of discrimination to the criminal justice system, encouraging surveillance, the imposition of stiffer penalties, etc., on minorities. When such records are made available to employers, discrimination in the hiring process is compounded. (See *Gregory* v. *Litton Systems.*)[42]

CONCLUSIONS AND RECOMMENDATIONS

LEAA is investing substantially in the creation of a national computerized criminal offender information file serving state and local contributors and users. The files at present contain too much information and are accessible to too many agencies, including private business concerns. Few safeguards protect legitimate rights of personal privacy or prevent use of the information in a discriminatory manner. Standing alone, the new information systems require immediate and comprehensive regulations and controls. The potential harm that they could inflict, however, is

[42] 316 F. Supp. 401 (C.D. Calif. 1970). The President's Commission on Federal Statistics, Vol. II (1971), p. 546, reported: "An applicant who lists a previous arrest faces at best a 'second trial' in which, without procedural safeguards, he must prove his innocence–at worst the listing of the arrest disqualifies him *per se*. The arrest record is the first of a series of 'status degradation ceremonies' in the criminal law process." The Commission pointed to the fact that in a recent survey of 39 countries not one lists arrests that have not led to convictions. "The 'criminal record' in these 39 countries includes only convictions, and often only those for serious crimes." (p. 548) For a detailed treatment of the problems inherent in the broad dissemination of arrest records, see *Security and Privacy of Criminal Arrest Records*, Hearings before Subcommittee No. 4 of the House Committee on the Judiciary, 92nd Congress, 2nd Session (April 1972).

made even more critical by (a) the coincident development of new state-level intelligence files on civil disorders and dangerous persons that are maintained by the same agencies that administer the information files and that are accessible to participants in the national system, and (b) the rapid expansion of computerized records on individuals maintained by welfare, health, education and other public and private agencies that can be (and have been) readily interfaced with the criminal offender files. To ensure integrity and fairness of such systems:

No further federal funds should be distributed for the operation, expansion or development of state and/or national information systems prior to the completion of a study by a neutral and reputable scientific body—such as the National Academy of Sciences or the National Commission on Individual Rights—setting forth the policy options facing the nation in regard to such systems. In particular, the study should examine: the necessity for various possible kinds of information (and intelligence) systems to effective law enforcement; the most appropriate structure(s) for such systems (centralized, decentralized, state controlled, law enforcement controlled, etc.); the kinds of safeguards that can and should be built into such systems; the relationship of the data banks developed under such systems to other data banks; and the proper forms for public regulation of such systems.

If a national or multi-state criminal justice information system is found to be justified after the full report by the independent body, federal legislation should be passed creating an affirmative right to privacy, which would require the government to justify in advance any activity that would conflict with that right. In addition, regulatory laws should be passed to control all information systems (1) developed and maintained by agencies of the federal government, (2) operated by state or local agencies but supported wholly or partly by federal funds and (3) interfacing with federal systems or federally supported systems. (If such legislation is not passed, the Attorney General should issue formal regulations under his present powers.) Among the kinds of safeguards that should be considered for inclusion in the legislation are the following:

- *The legislation should spell out with specificity (rather than defining by exclusion) the scope of the criminal history offender files and the matter to be included therein. Only serious crimes that pose actual danger to the public and are likely to involve interstate mobility should be included.*[43] *The national file should contain only identifying data, records of active arrests, convictions and sentencing and an identification of the state agency maintaining the full records. Records of arrests not followed by indictment or information within one year, or conviction within two years, should be deleted from the files. When a criminal law is repealed, the record of prior violations of it should be deleted from the computer. An affirmative obligation should be placed on all participating states to delete such information from their own files as well as the FBI files. Failure to do so should result in termination of participation in the system and imposition of financial penalties.*

- *Specific congressional approval should be required for any expansion or modification of the initial system, such as a decision to interface with other data banks within the Justice Department or other federal agencies.*

- *The legislation should provide for operation and/or monitoring of the national system by an independent agency or commission that would conduct audits and spot-checks on both the operating agency and the contributing agencies, and would report annually (and periodically, as requested) to Congress. The commission, which should include constitutional lawyers, representatives of citizens' groups and other civilians, would share responsibility with the operating agencies for the development of detailed guidelines to govern the operation of the system. No state should be allowed to participate in the federal system until such time as it has passed its own statute reflecting the national standards, creating a state monitoring body and providing for the protection of individuals whose records are included in the system.*

[43] This would remove most victimless crimes from the file as well as the other petty offenses that are most subject to enforcement patterns that are socially discriminatory.