Chapter 6

Legal/Regulatory Framework for NCIC, Ident, and State CCH Systems

Contents

TABLES

Chapter 6

Legal/Regulatory Framework for NCIC, Ident, and State CCH Systems

Chapter Summary

The management and use of criminal justice information in the United States are governed by a variety of Federal, State, and local statutes, regulations, and executive (or agency) orders, and Federal and State court rulings.

Overall, Federal statutes and regulations have:

- granted basic authority to the Attorney General and the Federal Bureau of Investigation (FBI) for operating its Identification Division (Ident) and the National Crime Information Center (NCIC);
- established standards for use of the various FBI criminal justice information systems.
- defined a range of authorized users of Federal systems (e.g., the Office of Personnel Management for Federal employee background checks by authority of Executive Order No. 10450); and
- established standards for use of State criminal history systems funded in whole or in part by the Law Enforcement Assistance Administration (LEAA).

During the 1970's, LEAA funding and the pioneering research of Project SEARCH (System for Electronic Analysis and Retrieval of Criminal Histories) played a significant role in stimulating substantial progress in development of State statutes and regulations for use of State criminal record systems. However, direct LEAA funding has now ended, and with it the option of terminating Federal funds for noncompliance (the primary penalty authorized by Congress).

In general, Congress has provided broad discretion to the FBI and LEAA in defining standards for the interstate collection, maintenance, and dissemination of criminal history information. Until the 1970's, title 28, United States Code (USC), sec. 534 provided the sole legislative direction at the Federal level. Congressional initiatives to pass comprehensive criminal justice information legislation in the early 1970's were not successful, but led to the enactment of an amendment to the Crime Control Act of 1973 requiring LEAA to issue detailed privacy and security regulations for State and local criminal history information systems (which appear as title 28, Code of Federal Regulations (CFR), pt. 20, subpt. B). Regulations for Federal systems (Ident and NCIC/CCH) and the interstate exchange of criminal history record information are set forth in title 28, CFR, part 20, subpart C.

The responsibility for enforcing management and use standards for criminal justice information is left largely up to the States, localities, and other users. For example, while LEAA regulations established standards for record quality and security, LEAA conducted little actual monitoring of State compliance, but did engage in an active program of publishing guidelines, model State codes, and the like.

While the FBI is authorized to terminate Ident and/or NCIC services to users who violate regulations, compliance is largely voluntary. At present, the FBI program to monitor compliance includes computer edits and quality checks of information from contributing agencies that is maintained in FBI files, but does not include direct audits of State or user files and record disseminations. Indeed, the FBI has never had the authority to conduct such audits.

In the early 1970's, efforts to enact comprehensive legislation, such as the "Criminal Justice Information Systems Security and Privacy Act of 1971" or the "Criminal Justice Information Control and Protection of Privacy Act of 1974, " were not successful; nor were initiatives in the late 1970's to include criminal justice information system standards as part of the proposed FBI charter legislation.

Federal Statutes and Regulations

Authority to Operate Ident and NCIC

The FBI has statutory authority to establish and maintain criminal history files in Ident and NCIC. (28 USC § 534 (1968)). In part, this statute authorizes the Attorney General to acquire, collect, classify, and preserve criminal identification, crime, and other records, and to exchange them with authorized officials of Federal, State, and local law enforcement agencies, and with penal and other institutions. The Attorney General has delegated this authority to the Director of the FBI in title 28, CFR, section 0.85. In addition, a 1973 amendment to the Omnibus Crime Control and Safe Streets Act of 1968, Public Law No. 90-351, 82 Stat. 200 (1968), adding a section 524 (42 USC § 3771), directs the executive branch to assure the adequate provision of privacy and security of criminal history information (reorganized by Public Law No. 96-157, § 818,93 Stat. 1212 (1979) as 42 USC § 3789g (Supp. 1980)). The privacy and security regulations in 28 CFR part 20 (1975) were issued pursuant to this congressional directive.

Record Content

The information that may be stored in criminal history records maintained by Ident and NCIC is described in 28 CFR § 20.2 (1975), and includes identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, and details as to sentencing, correctional supervision, and release. Only information on serious and/or significant offenses may be stored in these records (28 CFR § 20.32, 1975). Specifically excluded are the nonserious offenses of drunkenness, vagrancy, disturbing the peace, curfew violation, loitering, false fire alarm, nonspecific charges of suspicion or investigation, and traffic violations (other than manslaughter, driving under the influence of drugs or liquor, and hit and run). Offenses committed by juvenile offenders are also specifically excluded unless the juvenile is tried in court as an adult.

Menard v. Saxbe, 498 F.2d 1017 (1974) resulted in judicial examination of the content of the FBI's criminal history files. It involved a suit against the FBI for expungement of a State (California) arrest record retained by the FBI. It had been established at the State level that there was no probable cause for the arrest, and the status of the proceeding was changed from "arrest" to "detention." The FBI had been so notified, and had amended its record to show that the subject encounter with the police was not considered to be an arrest under California law, and that no formal proceedings had been brought. The court determined that once the FBI was notified that the subject was not involved in the criminal justice process, it had no authority to retain the record in the criminal files, even though the record accurately portrayed the events as they had occurred. The controlling statute (28 USC § 534) only authorizes the storage of information about formal criminal proceedings in the criminal files. The court stated that the FBI has a responsibility to assure that it does not disseminate criminal records containing inappropriate information. The decision was

'This section is based on app. A to Jet Propulsion Laboratory, *FBI Fingerprint Identification Automation Study: AIDS III Evaluation Report Volume VI: Environmental Analysis,* California Institute of Technology, Pasadena, Nov. 15, 1980, prepared for the L'. S. Department of Justice, Federal Bureau of Investigation.

carefully grounded on statutory considerations, but the court left as an open question the extent to which this decision is mandated by the U.S. Constitution.

One unresolved problem that arises from this decision is what to do with the fingerprints of suspects who undergo pretrial diversion. This alternative to the usual judicial process is sometimes used when the U.S. Attorney determines that the suspect's infraction of the law was due to an unfortunate set of circumstances and is not likely to be repeated. Sometimes the suspect is formally arrested, sometimes not. Instead of going through the usual criminal process, the suspect agrees to a set of conditions, which usually involve some type of restitution to the victim and a period of probation. If these obligations are successfully fulfilled, the charges are either dismissed or never brought. The unresolved question is whether pretrial diversion qualifies as a formal criminal process under 28 USC § 534 when the suspect is not actually arrested. The FBI retains such records now, but its authority to do so is uncertain after the Menard decision. The FBI has requested legislative direction in this matter, but so far none has been forthcoming.

Record Updating

On May ***20, 1975,*** the Department of Justice (DOJ) issued a regulation prohibiting dissemination of arrest information more than a year old unless accompanied by a disposition when no active prosecution of the charge is known to be pending (28 CFR § 20.33, 1975). The prohibition does not apply to records released for criminal justice purposes or to authorized Federal agencies. It came in the wake of *Tarleton v. Saxbe 507* F.2d 1116 (1974) in which the court expressed concern about the impairment of an individual's liberty that results when that person stands accused of a crime. It noted that the reason for the constitutional guarantee of a speedy trial is to mitigate this restriction of the accused's liberty, and the court suggested that the lower court inquire into what justifications, if any, exist for the FBI's failure to indicate dispositions within a reasonable time after arrest. Two years later, the district court order in *Tarleton v. Saxbe* ***407*** F. Supp. 1083 (1976) directed the FBI to conduct a feasibility study of system procedures that would enable it to keep disposition entries in its criminal records reasonably current. By the time the study was conducted, the FBI had solved the immediate problem by promulgating 28 CFR § 20.33 (1975). Most of the systems and procedures suggested by the study for keeping the disposition data more current were designed for use in a computerized system.

Regulation 28 CFR § 20.37 (1975) makes it the responsibility of each criminal justice agency contributing data to FBI criminal history record information systems to assure that information is kept complete, accurate, and current. It calls for a disposition to be submitted within 120 days after it has occurred. However, the only sanction available for enforcing this policy is regulation 28 CFR § 20.38 (1975) that permits DOJ to cancel its criminal record services to any agency that fails to comply with its regulations.

Pursuant to 28 CFR § 20.32 (1975), Ident and NCIC do not record minor and juvenile offenses. Although this regulation went into effect in June 1975, NCIC has had such a policy since November 29, 1971, and Ident since February 9, 1973. The regulation itself does not require the FBI to expunge information on minor offenses previously compiled. However, the district court's order in *Tarleton v. Saxbe 407* F. Supp. 1083 (1976) required the FBI to delete from the record, prior *to dissemination, all* information relating to nonserious offenses. The FBI *is* deleting these offenses from requested records as they are sent out.

The FBI currently expunges and seals records pursuant to State and Federal court orders. The authority for sealing the record of a person who has been found guilty of unlawful possession of a controlled substance is found in 21 USC § 844(b)(1) (1972). If the subject individual has not previously been convicted of violating any Federal narcotics laws, the court may, after trial or entry of a guilty plea, place the person on probation without entering a

judgment of guilty. If the person does not violate any conditions of the probation, the court may dismiss the proceedings. DOJ retains a record solely to determine first offender status.

As of July 1981, 35 States provide procedures whereby subjects can have nonconvictions purged from their records, and 24 provide a procedure for purging records of convictions. Twenty States provide for sealing of records of nonconviction and 22 provide for sealing of convictions.[2] For example, Arkansas provides for purging "all records . . . relating to a crime wherein the person has been acquitted or the charges dismissed" (Ark. Stat. Ann. § 5-1109, 1975). This State also provides for the sequestering of records of first offenders so that they are available only to law enforcement and judicial officials (Ark. Stat. Ann. § 43-1231, 1975). When either procedure takes place, the court sends a copy of the order to the Arkansas State Identification Division and the FBI Identification Division. In comparison, the California Penal Code allows a defendant who has been acquitted to file a motion to seal rather than purge the record of arrest and acquittal (Cal. Penal Code § 851.8, Deering Supp., 1980). As in Arkansas, a copy of the judge's order sealing the record is forwarded to law enforcement agencies, including the FBI.

On September 24, 1973, DOJ instituted (by DOJ Order 556-73) a procedure by which individuals, upon request and verification of identity, may review the criminal history information maintained on them. Individuals may apply to the contributor of the information to make any changes in the record. If the contributor corrects the record it must notify the FBI, and the FBI will make any changes necessary in accordance with the corrections (28 CFR § 20.34, 1975).

Record Dissemination

Recipients of criminal history information are limited by 28 USC § 534 (1968) to law enforcement agencies, penal, and other institutions. In 1971, the district court for the District of Columbia, in deciding Menard v. *Mitchell 328* F. Supp. 718 (1971), held that "other institutions" refer to other official criminal justice and law enforcement institutions only. Prior to this decision, the FBI had been providing criminal history records to States for employment and licensing checks. Immediately after this decision, Congress responded by passing the Departments of State, Justice, and Commerce, the Judiciary, and Related Agencies Appropriation Act, 1973, Public Law No. 92-544, § 2, 86 Stat. 1109 (1972) allowing the FBI to disseminate criminal history information to officials of federally chartered or insured banking institutions. Public Law No. 92-544 also permits dissemination to State and local government agencies for purposes of employment and licensing if the check is authorized by a Federal or State statute and approved by the Attorney General.

Then, in 1975 Congress amended the Securities Exchange Act, § 17 (15 USC 78q(F)(2)) to require every member of a national securities exchange, and every broker, dealer, registered transfer agent, and registered clearinghouse agency to undergo an FBI criminal history check.

The dissemination of criminal histories to authorized Federal agencies is permitted pursuant to Federal statute or Executive order, 28 CFR § 20.33(2) (1975). For example, Executive order 10450 requires a national security investigation of prospective civilian officers or employees in any department or agency of the Federal Government. In most cases the investigation includes at least a national agency check (including a check of FBI files) and written inquiries to local law enforcement agencies. In effect, the order authorizes dissemination of criminal history record information to Federal agencies for use in background investigations, whether national agency checks or full field investigations. This authority has also been established for military employees or applicants (Executive order 12065) and for certain employees of defense contractors (Executive order 10865).

[2] SEARCH Group, Inc., *Trends* in *State Security and Privacy Legislation,* Sacramento, Calif., November 1981, p. 5, prepared for the U.S. Department of Justice, Bureau of Justice Statistics.

As a consequence of *Menard v. Mitchell*, DOJ has strictly construed the statutes governing dissemination of criminal history files. It has revised its earlier position under 28 USC § 534 (1968) and now refuses to allow access, directly or through State law enforcement agencies, to railroad police and campus police. Even though these groups may be authorized by State statute to investigate crimes or apprehend criminals, DOJ does not find them to be authorized Government officials under the meaning of 28 USC § 534. It has also refused, under Public Law 92-544, to provide criminal history records to State boards of bar examiners when the board is established by rule of the State supreme court rather than by a statute.

Once the criminal history records leave the FBI's control, one sanction available to enforce FBI dissemination policies is 28 CFR § 20.33 (b)(1975). This regulation provides that the exchange of criminal history record information with authorized recipients is subject to cancellation if dissemination is made outside the receiving department or related agencies. Also, certain civil and criminal penalties are provided under the Privacy Act of 1974.

Freedom of Information and Privacy Act

Under the Freedom of Information Act, Public Law No. 89-487, 80 Stat. 250 (codified at 5 USC § 552, 1977), all Government agencies are required to supply copies of their records to any member of the public who requests them (5 USC § 552(a)(3)). It has been established that this act applies to computer tapes to the same extent that it applies to other records *(Long v. U.S. IRS* 596 F.2d 362, 1979). However, the act provides several categories of exemptions: 1) matters that are exempt under another statute, if the statute leaves the agency no discretion or supplies particular criteria for applying the exemption, may be withheld from the public (5 USC § 552(b)(3)); 2) if disclosure of a file would constitute "a clearly unwarranted invasion of personal privacy" it need not be disclosed (5 USC § 552(b)(6)); and 3) investigatory records compiled for law enforcement purposes are exempt if release would constitute "an unwarranted invasion of personal privacy" (5 USC § 552(b)(6C). Note that the privacy standard for these records is less strict than the privacy standard for other records. There are other exemptions covering law enforcement records, but they are of limited application (see 5 USC § 552(b)(7)). If the agency invokes any one of these exceptions, it must release any reasonably separable portion after deleting the exempt portions.

Regulations promulgated pursuant to this statute allow the Attorney General to exempt the whole system of FBI criminal records from public disclosure. This exemption, which is noted in DOJ regulations (28 CFR § 16.10, 1973), is uniformly applied to exempt all criminal histories from disclosure.

The Privacy Act of 1974 (Public Law 93-579 codified in part at 5 USC § 552a, 1977) was passed shortly after the Freedom of Information Act. Its purpose is to protect the privacy interests of individuals by regulating the collection, maintenance, use, and dissemination of personal information by Federal agencies. The Privacy Act requirements apply to all Federal agency systems including Ident and NCIC, except where the head of an agency (in this case the Attorney General) may exercise certain exemptions for systems of records maintained for the enforcement of criminal laws. The Attorney General has exercised specific exemptions, particularly for access and challenge procedures. However, alternate procedures are provided in 28 CFR § 20.34, which establishes the right of individuals to have access to and review their own criminal history record information maintained by Ident or NCIC, and to seek correction by the source agency if the information is believed to be incorrect or incomplete. Individuals may also direct a record challenge to the FBI, who will then forward the challenge to the source agency. The FBI will make any changes necessary in the Ident or NCIC files if proper notification is received from the source agency.

NCIC Operating Policies and Procedures

The FBI Director has approved a set of NCIC operating policies and procedures; these embody the statutory-regulatory framework discussed above, but go considerably further in some areas. The policies and procedures are based in part on recommendations from the NCIC Advisory Policy Board, and are included in the NCIC Operating Manual distributed to NCIC terminal operators. The manual is updated and revised periodically as needed.

Selected NCIC Hot File Operating Procedures

Each record in an NCIC file is identified with the originating agency. The NCIC Operating Manual emphasizes repeatedly that "agencies that enter records into NCIC are responsible for record accuracy, timeliness, and completeness."3

The FBI does assume responsibility for those records entered by the FBI. In addition, "the FBI—as system manager—helps maintain the integrity of the system through: 1) automatic computer edits that reject certain types of errors in data; 2) automatic purging of records after they are on file for a prescribed period of time; 3) quality control checks by FBI personnel; and 4) periodically furnishing lists of all records on file for validation by the originating agencies."4

The manual also emphasizes that "an NCIC 'hit' may not be probable cause for arrest. " NCIC only provides one more piece of information to be evaluated by the officer along with other facts in determining if there is sufficient legal basis for probable cause to arrest a person or seize property.[5] An immediate confirmation with the originating agency "is necessary to ensure the validity of the hit before an arrest or seizure is made. " The manual points out that "NCIC is an informational tool. It is no substitute for professional judgment. " NCIC information must be evaluated along with other facts known to the criminal justice official. Finally, NCIC procedures place some limitations on what can be entered into files. For example, before entering a record into the wanted persons file, the entering agency is required to determine, to the maximum extent possible, if extradition will be authorized. If not, the record should not be entered.[G]

The manual further provides detailed procedures for correcting errors and for sending and receiving messages with the various hot files.

Selected CCH File Operating Procedures

As with the NCIC hot files, each criminal justice agency contributing data to CCH is responsible for assuring that information on individuals is kept complete, accurate, and current. For all arrest data included in such records, disposition data should also be included "to the maximum extent feasible" and submitted to CCH within 120 days after the disposition has occurred.[7]

Unlike the hot files, CCH operating procedures require that all criminal justice agencies seeking direct access to CCH execute a written agreement with the FBI Director. This agreement commits the agency to abide by all CCH rules, policies, and procedures.[8] These procedures were approved by the NCIC Advisory Panel Board and adopted by the FBI Director.

The CCH operating procedures specify the kinds of criminal history information that may be entered into the CCH file, require continuous checks by the FBI and States on the accuracy of records in the file, and define the right of an individual with a record in the CCH file to review that record and seek correction if the information is believed to be inaccurate or in-

[3] *NCIC Operating Manual "Introduction,* p. 7.
[4] Ibid.
[5] 1 bid., p. 2.
[6] Ibid., p. 7.
[7] Ibid., pt. 10, p. 7, same as 28 CFR § 20.37.
[8] Ibid., same as 28 CFR § 20.36.

complete. In addition, they also define who may have direct access to CCH records and the limitations on the use of such records.

With respect to system security, systems that interface directly with NCIC are required to be under the management control of criminal justice agencies. The procedures also establish a set of physical, technical, and personnel security measures required of all agencies having access to CCH. These measures include logging all transactions against the CCH file, screening and verifying all CCH inquiries, placing all terminals in secure locations, and screening all terminal operators.

Finally, the procedures define the role of the NCIC Advisory Policy Board, particularly with regard to establishing criteria for purging records, for secondary access to CCH, and for the organization and administration of CCH. With respect to the last, all rules governing direct terminal access to the CCH file apply equally to Federal and State agencies. In addition, such agencies must permit an Advisory Board-appointed inspection team to conduct inquiries concerning any alleged security violations.[9]

Federal Agency Orders or Procedures

In addition to the NCIC operating policies and procedures, some Federal agencies have their own orders or procedures for using NCIC. OTA conducted a partial survey of Federal users to identify the range of operating policies and procedures that govern the use of NCIC. Illustrative results of this survey are summarized in table 11.

[9] For further details, see Ibid., pp. 15-27.

Table 11.—Federal Agency Orders or Procedures for NCIC

Agency	Policy/procedure
Bureau of Indian Affairs (BIA) U.S. Department of the Interior[a]	None. Adheres to policies and procedures of agency operating terminal.
Internal Revenue Service (IRS) U.S. Department of the Treasury[b]	Both Criminal Investigative Division (CID) and Internal Security Division (IS) have detailed operating procedures, e.g., CID procedures require NCIC be queried when evaluating possible tax fraud. NCIC entries are limited to IRS fugitives, and permitted only at the CID National Office terminal in Washington, D.C. Fugitives are purged from NCIC when apprehended or when matter is dismissed by Federal courts.
Postal Inspection Service U.S. Postal Service[c]	Part 11, ch. 1, sec. 18 of *Confidential/ Field Manual.* Authority provided by 39 USC § 404(a)(7) and 18 USC § 3061. NCIC access by written agreement with FBI.
Federal Prison System (FPS) U.S. Department of Justice[d]	FPS program statements 1070.1 and 1231.1 and NCIC operating manual.
United States Marshals Service U.S. Department of Justice[e]	USM Order 2423.1, ch. 3; e.g., arrest warrants issued to U.S. Marshal by a Federal court are to be screened to determine if the USMS retains the primary responsibility for their entry into NCIC. Warrant information will be forwarded via Justice Telecommunication System (JUST) within 48 hours to the USMS Communications Center for entry into NCIC according to the NCIC operating manual,

a Oct 16, 1979, memorandum to OTA from Division of Law Enforcement Services, Bureau of Indian Affairs, U S Department of the Interior
b Oct 2, 1979, letter to OTA from Deputy commissioner, Internal Revenue Service, U S Department of the Treasury
c Dec 24, 1979, letter to OTA from the Chief Postal Inspector, U S Postal Service
d Sept 18, 1979, memorandum to OTA from the Director, Federal Prison Service, U.S Department of Justice
e Sept 18, 1979, memorandum to OTA from Director, U S Marshals Service, U S Department of Justice

SOURCE Off Ice of Technology Assessment

Federal and State Court Rulings

State and Federal courts have focused primarily on the collection, use, and maintenance of identification and arrest records by police at the local and State levels. As discussed ear-

lier, some more recent cases (e.g., *Menard v. Saxbe, Tarleton v. Saxbe, Menard v. Mitchell)* have begun to focus on the recordkeeping policies and practices of the FBI.

In general, however, the activity of the State and Federal courts has been infrequent and uncertain throughout the 100-year history of law enforcement and criminal justice recordkeeping. Judicial rulings have lacked a consistent direction, as illustrated in table 12. '0 This is

[10] For further discussion of judicial rulings, see Donald A Marchand, et al., *History and Background Assessment of the National Crime Information Center and Computerized Criminal History Program,* Bureau of Governmental Research and Service, University of South Carolina, June 1979, sec. V, "Regulating the Use of Criminal History Records in the United States: Overview of Activities, " pp. 168-175.

Table 12.—Illustrative Federal/State Court Rulings on Criminal Records

Year	court	Case	Ruling	Individual rights	Public safety and welfare
1906	Supreme Court Louisiana	Itzkovitch *v. Whitaker*	**Ruled for the defendant.** Police could not post picture in rogues' gallery since it violated defendant's personal rights because he had never been convicted.	x	
1941	Supreme Court Missouri	*State v. Harris*	Kansas City Police restrained from disseminating photographs and fingerprints of defendent within State and nationwide.	X	
1944	court of Chancery New Jersey	*Fernicola v. Keenan*	In absence of controlling statute, police had discretion to destroy fingerprints, photographs, and measurements of those accused but not convicted,		x
1945	Court of Chancery New Jersey	McGovern v. *Van Riper*	No justification for taking identification records in advance of conviction, except to identify person charged or to recapture a fugitive.		
1946	Supreme Court Indiana	*State v. Tyndall*	Absent a statute, police had discretion to maintain and operate record systems for identification, even for those acquitted of misdemeanors.		x
1966	U.S. Court of Appeals	*Herschel v. Dyra*	Absent State statute, police could retain arrest records whether accused was acquitted, discharged, or released.		x
1967	US. Court of Appeals Alabama	*U.S. v.* McLeod	County officials should return fines and expunge police and court records connected with arrests and prosecutions intended to intimidate black citizens who wished to vote.		
1967	US. District Court Puerto Rico	*U.S. v Kalish*	Ordered fingerprints and photographs destroyed that were taken when defendant was arrested for refusing to submit to military induction.		
1968-72		(a)	Decisions generally favored defendants involved in illegal and mass arrests or arrests not leading to conviction. Generally aimed at local or State police departments, not Ident.		
1970	U.S. Court of Appeals District of Columbia	*Menard v. Mitchell*	Arrest alone did not justify maintenance of fingerprints or record by State or Ident.		
1971	U.S. District Court District of Columbia	*Menard v, Mitchell*	Where probable cause for arrest exists, court would not order expungement by FBI, but would limit disclosure to nonlaw enforcement officials for employment purposes.		x
1974	U.S. Court of Appeals District of Columbia	*Menard v, Saxbe*	FBI had no authority to retain record since "arrest" was changed to "detention, " FBI could retain "neutral identification records. "		
1974	U.S. Court of Appeals District of Columbia	*Tar/ton v. Saxbe*	FBI had duty to prevent dissemination of inaccurate arrest and conviction records, and had to take reason. able precautions to prevent inaccuracy and incompleteness of records,		
1976	U.S. Supreme Court	Paul v, *Davis*	Court held that the police had a right to publicize a record of an official act, such as an arrest, without exposing State or Federal officials to lawsuits for civil rights invasion.		x
1979	U.S. District Court New York	Tatum v. *Rogers*	Court found a violation of sixth, eight, and 14th amendment rights when arrest information without otherwise available disposition was used in setting bail.	x	

See, for example, *Hughes v. Rizzo,* **282 F** Supp. **881 (1968),** *Morrow v District of Columbia, 417* F 2nd 728 (1989), *Wheeler v* **Goodman, 306 F Supp 58 (1969)**

SOURCE Office of Technology Assessment.

due in part to the limited involvement of the U.S. Supreme Court in this area. Most of the significant decisions have been made in State and lower Federal courts, and have varied widely in different States. Any trends in judicial decisionmaking have been more a product of the larger social and political movement toward expanding due process and other individual rights over the last 40 to 50 years, rather than the result of changes in judicial perspectives on criminal justice recordkeeping per se.

In most criminal record cases, the balancing of individual rights of privacy and due process versus the maintenance of public safety and welfare has proven to be a difficult challenge to the courts. The tools that the courts have had at their disposal, such as injunctive relief and court orders to seal and expunge specific records, have been of limited effectiveness and used reluctantly. The courts have frequently sought legislative guidance.

State Statutes and Regulations

The last 10 years have seen a dramatic increase in State statutes and regulations on criminal justice information systems. This is partly owing to the development of LEAA regulations (title 20, CFR, pt. 20) and State efforts to implement them.

Early Efforts of Project SEARCH and LEAA

In 1970, Project SEARCH (originally the System for Electronic Analysis and Retrieval of Criminal Histories) with LEAA funding developed a series of guidelines, model State statutes, and model administrative regulations for State and local CCH systems.[11] This effort was premised on the view that a nationally integrated CCH should be federated in nature; i.e., fundamentally dependent on State and local systems as opposed to one uniform national system. However, Project SEARCH recognized that such an approach would necessitate privacy and security standards at the State and local as well as Federal levels to uniformly protect individual rights and mitigate potential adverse social impacts.

These early voluntary efforts produced some results. For example, four States—Alaska, California, Iowa, and Massachusetts–adopted the model State act and/or regulations in whole or in part. At the local and regional level, codes of ethics and self-imposed guidelines were adopted by some systems, such as the Santa Clara County (California) criminal justice information system and the Kansas City (Kansas) Alert II regional system."

However, in 1971, concerned about the still limited acceptance of the Project SEARCH standards, LEAA required State plans to include provisions for privacy and security. In 1972, LEAA established the Comprehensive Data System (CDS) program that provided Federal dollars for CCH development, but made privacy and security plans a condition of funding.

The CDS program was the primary means for LEAA to tie the development of local and State criminal justice information systems to a set of minimum standards for system development, privacy, and security. In July 1973, the LEAA-sponsored National Advisory Com-

"See Project SEARCH, Security *and* Privacy *Considerations in Criminal History Information Systems,* California Crime Technological Foundation, Sacramento, 1970; and *A Model State Act for Criminal Offender Record Information,* California Crime Technological Foundation, Sacramento, 1971. Also see Project SEARCH Committee on Security and Privacy, *Model Adrninistrative Regulations for Criminal Offender Record Information,* March 1972.

"See Donald Marchand, *Criminal Justice Records and Civil Liberties: The State of California,* Department of Justice, State of California, Sacramento, 1973, pp. 136-138, 358-366; and Melvin F, Bockelman, "ALERT II–Progress Toward a Computerized Criminal Justice System, " in Project SEARCH, *Proceedings of the International Symposium on Criminal Justice Information and Statistics Systems,* California Crime Technological Foundation, Sacramento, Calif., 1974, pp. 126, 131-2.

81-048 O - 82 - 4

mission on Criminal Justice Standards and Goals adopted privacy and security standards that largely reflected Project SEARCH reports.'[13] By March 1974, 33 States had indicated their desire to participate in the CDS program by submitting plans. "

Implementing LEAA Privacy and Security Regulations

In 1973, an amendment was added to the Omnibus Crime Control and Safe Streets Act of 1968 by Sen. Edward Kennedy requiring LEAA to promulgate regulations to provide safeguards for the privacy and security of criminal history record information. The Kennedy amendment followed a period of frustrating efforts by both the House and the Senate to pass legislation controlling the use of arrest records nationwide.

During July 1973, Senator Kennedy "tacked on" his amendment to the primary piece of legislation supporting the LEAA program. While the measure was considered temporary by Congress in the light of anticipated efforts to pass more comprehensive legislation, it had considerable impact on LEAA and its relations with State and local criminal justice agencies.

Section 524(b) of the Crime Control Act of 1973, as amended, provided that:

> All criminal history information collected, stored, or disseminated through support under this title shall contain, to the maximum extent feasible, disposition as well as arrest data where arrest data is included therein. The collection, storage and dissemination of such information shall take place under procedures reasonably designed to insure that all such information is kept current therein; the Administration shall assure that the security and privacy of all information shall only be used for law enforcement and criminal justice and other lawful purposes. In addition, an individual who believes that criminal history information concerning him contained in an automated system is inaccurate, incomplete, or maintained in violation of this title, shall, upon satisfactory verification of his identity, be entitled to review such information and to obtain a copy of it for the purpose of challenge or correction.[15]

Following passage of the act with the Kennedy amendment, LEAA issued draft regulations in 1974 and held hearings in different parts of the country. On May 20, 1975, LEAA published its regulations, which required States accepting Federal funding to develop specific policies and procedures in five areas: 1) completeness and accuracy of records, 2) audit, 3) individual access and review, 4) limits on dissemination of records, and 5) security.[16]

LEAA issued final regulations on March 19, 1976. The States experienced a number of problems in implementing the regulations including lack of resources, confusion in interpretation of the regulations, and lack of a State legislative mandate." More specifically, the following impediments to State implementation were identified in each of the five areas covered by the regulations:

- *Completeness and Accuracy:* the lack of a clear and effective mandate, funds and/or technical ability needed to introduce or improve an arrest and disposition reporting system, and sufficient time in which to do SO.
- *Individual Access and Review:* the lack of standardized, comprehensive policies, applicable to all impacted agencies in a State, which are supported by formalized procedures and the force of State law.
- *Limitations on Dissemination:* the lack of a statewide policy supported by formal-

---

[13] National Advisory Commission on Criminal Justice Standards and Goals, *Report on the Criminal Justice System,* U.S. Government Printing Office, Washington, D, C., 1973.

[14] Richard W. Velde, LEAA Deputy Administrator for Policy Development, prepared statement in U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Constitutional Rights, *Criminal Justice Data Banks, Hearings,* vol. I, 93d Cong., 2d sess., 1974, p. 301.

[15] "Omnibus Crime Control and Safe Streets Act of 1968, Public Law 90-351,82 Stat. 200 (1968), adding sec. 524 (42 USC § 3771). Carried forward by Justice Systems Improvement Act of 1979, Public Law 96-157, § 818, 93 Stat. 1212 (1979) as 42 USC § 3789g (Supp. 1980).

[16] "Codified in 28 CFR 20, subpt. B.

"See Mitre Corp., *Implementing the Federal Privacy and Security Regulations,* McLean, Va., December 1977.

ized mechanisms and procedures, that is promulgated, pursued and enforced by some responsible agency.

- *Security:* the lack of specific, statewide security standards and the resources required for the full implementation of these standards.
- *Audit:* the lack of both a legislative mandate to conduct audits and the resources these audits will require. '8

In 1978, LEAA issued two publications to assist the States in adopting information management policies for local and State criminal justice information systems. The first surveyed in detail the existing privacy and security statutes and administrative policies.[19] The second assessed the issues and difficulties that the States have confronted in 25 areas of information policy, and highlighted 4 State approaches to developing regulations.[20] In addition, LEAA and SEARCH Group, Inc. (a nonprofit corporation formed in 1975 with broader membership and interests than the original Project SEARCH) continued to provide policy, management, and technical assistance to State and local agencies. However, by 1980 almost all LEAA funding for State implementation had been phased out. LEAA itself was reorganized by the Justice Systems Improvement Act of 1979, with most prior functions terminated or transferred to other agencies by spring 1982. SEARCH Group, Inc. continues to receive research funds from DOJ Bureau of Justice Statistics.

State Statutes and Regulations as of June 1981

The latest comprehensive survey of State statutes and regulations, conducted by SEARCH Group, Inc., and funded by the Bureau of Justice Statistics, documents substantial progress between 1974 and mid-1981.[2,] State statutes and regulations are classified into 28 different categories described in table 13.[22] The methodology used to conduct this and similar prior surveys "included library research and extensive contact with both the legislative information offices and record repositories of many States. Once the laws were collected, each State's Attorney General was sent a copy of his State's laws and attested to their completeness and accuracy. Responses served to correct any omissions or inaccuracies in the initial survey. "[23]

The survey results are summarized in table 14. They indicate that by 1981 over two-thirds of the States had statutes and/or regulations: 1) establishing a State regulatory authority (46 States in 1981 compared with 7 States in 1974); 2) placing some kind of restrictions on dissemination of criminal history information (51 States compared with 12 States); 3) establishing the rights of individuals to inspect their criminal history records (43 States compared with 12); 4) requiring agencies to ensure reasonably complete and accurate criminal history information, including timely disposition reporting (49 States compared with 14); 5) providing criminal sanctions for violation of privacy and security laws (39 States compared with 18); and 6) stipulating what criminal history records are to be open to the public (52 States in 1981 compared with 9 in 1974).

— — —

"Ibid., *Volume 1: Findings and Recommendations of an Eighteen State Assessment,* p. ix.

[19]LEAA, U.S. Department of Justice, *Privacy* and *Security of Criminal History Information: A Compendium of State Legislation,* 1978.

[20]LEAA, U.S. Department of Justice, *Privacy and Security of* **Criminal** *History Information: An Analysis of Privacy Issues, 1979.*

"SEARCH Group, Inc., *Trends in State Security and Privacy Legislation,* Sacramento, Calif., November 1981. The full results of the survey are available from the Bureau of Justice Statistics, U.S. Department of Justice.

"These are the same 27 categories used in the 1978 LEAA *Compendium of State Legislation* and a 1979 Supplement, with the addition of category 28, "Establishment of a Central State Repository. "

[23]LEAA, Ibid., 1979 Supplement, p. vii.

Table 13.—Categories of State Statutes and Regulations

1. State Regulatory *Authority.* —A grant of power to a State agency to promulgate Statewide security and privacy regulations for criminal justice information systems.
2. *Privacy and Security Council.* —A State board, committee, commission, or council whose primary statutory function is monitoring, evaluating, or supervising the confidentiality and security of criminal justice information.
3. *Regulation of Dissemination.* —Restrictions on dissemination of criminal history information.
4. Right *To Inspect.* —The right of an individual to examine his criminal history records.
5. *Right To Challenge.* —The right to an administrative proceeding in which an individual may contest the accuracy or completeness of information pertaining to him.
6. *Judicial Review of Challenged Information.* —The right of an individual to appeal an adverse agency decision concerning challenged information to a State court.
7. *Purging.' Nonconviction* Information.—The destruction or return to the individual of criminal justice information where no conviction has resulted from the event triggering the collection of the information.
8. *Purging: Conviction /n formation.* —The destruction or return to an individual of criminal history information indicating a conviction.
9. *Sealing: Nonconviction Information.* —The removal of criminal history information from active files where no conviction has resulted from the event triggering the collection of information.
10. *Sealing: Conviction Information.* —The removal from active files of individual criminal history information indicating a conviction.
11. *Removal of Disqualifications.* —The restoration of rights and privileges such as public employment to persons who have had criminal history records purged or sealed.
12. *Right To State Nonexistence of a Record.* —The right to indicate in response to public or private inquiries the absence of criminal history in cases of arrest not leading to conviction or where an arrest or conviction record has been purged.
13. *Research Access.* —The provision for and regulation of access to criminal justice information by outside researchers.
14. *Accuracy and Completeness.—A* requirement that agencies institute procedures to ensure reasonably complete and accurate criminal history information, including the setting of deadlines for the reporting of prosecutorial and court dispositions.
15. Dedication. The requirement that computer configurations be assigned exclusively to the criminal justice function.
16. *Civil Remedies.* —Statutory actions for damages or other relief resulting from violations of various privacy and security laws.
17. Criminal Penalties.—Criminal sanctions for a violation of various privacy and security laws.
18. *Public Records.* —Requirements that certain criminal history records maintained by the police or courts be open to the public.
19. *Separation of Files.* —Requirements that criminal history information be stored separate from investigative and intelligence information.
20. Regulation of Intelligence Collection, —Restrictions on the kind of intelligence information that may be collected and retained and/or prohibition on its storage in computerized systems.
21. *Regulation of Intelligence Dissemination.* —Restrictions on dissemination of intelligence information.
22. *Security.* —Requirements that criminal justice agencies institute procedures to protect their information systems from unauthorized disclosure, sabotage, and accidents.
23. *Transaction Logs.* —Records that must be maintained by criminal justice agencies indicating when and to whom criminal justice information is disseminated.
24. *Training of Employees.* —Security and privacy instruction that must be provided to employees handling criminal justice information.
25. *Listing of /formation Systems.* —A mandatory disclosure of the existence of all criminal justice information systems describing the information contained in such systems.
26. *Freedom of Information (Including Criminal Justice Information).* —Provisions for public access to government records that apply to criminal justice records.
27. *Freedom of information (Excluding Criminal Justice in*formation). —Provisions for public access to government records from which criminal justice records are specifically excluded.
28. *Central State Repository.* Establishment of a bureau, agency, or other entity to collect and maintain criminal history records or criminal identification data for all criminal justice agencies in the State.

SOURCE SEARCH Group, Inc , LEAA, and Bureau of Just Ice Statistics

Table 14.—Survey Comparison of Changes in State Statutes/Regulations by Category[a]

Item	1974	1977	1979	1981
1. State regulatory authority ...	7	38	42	46
2. Privacy and security council	2	10	13	21
3 Regulation of dissemination .	24	40	44	51
4 Right to Inspect	12	40	43	43
5. Right to challenge	10	30	36	35
6. Judicial review of challenged information	10	20	22	18
7 Purging nonconviction information	20	23	28	35
8. Purg!ng conviction Information	7	13	19	24
9 Sealing nonconviction information	8	15	16	20
10 Sealing conviction information	7	20	21	22
11 Removal of dlsqualifications	6	22	22	27
12 Right to state nonexistence of a record .	6	13	17	22
13 Researcher access. ... ., .,	6	12	14	21
14, Accuracy and completeness	14	41	45	49
15 Dedication	2	3	3	2
16. Civil remedies ., ...	6	22	25	33
17. Criminal penalties	18	35	39	39
18, Public records	9	43	42	52
19 Separation of files ... .,	5	10	10	7
20. Regulation of intelligence collection. . .	3	10	10	13
21. Regulation of intelligence dissemination	7	24	25	19
22, Security	12	26	31	32
23. Transaction logs . . . . . .,	6	11	27	29
24. Training of employees. . . . .,	4	18	23	16
25. Listing of Information systems	1	8	8	8
26. Freedom of Information Including Criminal Justice	(b)	(b)	18	27
27. Freedom of Information excluding Criminal Justice	(b)	(b)		22
28. Central State repository . .	(b)	(b)	(')	52

[a]The figures presented are cumulative and may include statutes or regulations previously enacted but excluded from prior surveys
[b]Data unavailable for these years

SOURCE SEARCH Group, Inc, Bureau of Justice Statistics and LEAA, U.S Department of Justice

Initiatives to Enact Comprehensive Federal Legislation[24]

As noted earlier, the Kennedy amendment to the Omnibus Crime Control and Safe Streets Act of 1973, and more recently the restrictions on NCIC hardware procurements and prohibitions on FBI message switching included in DOJ Appropriations Acts, have been interim actions aimed at dealing with spe cific problems until more comprehensive legislation could be enacted. During the decade-long debate, congressional initiatives and executive branch proposals for comprehensive legislation on criminal justice information systems have not produced such legislation.

As early as 1970, Congress approved an amendment to the Omnibus Crime Control and Safe Streets Act, sponsored by Sen. Charles Mathias, which required LEAA to submit legislation to ensure the integrity and accuracy of criminal justice information systems funded in whole or in part by the Federal Government, and protecting the constitutional rights of all persons covered *or* affected by the act. In 1971, Sen. Roman Hruska introduced S. 2546, "The Criminal Justice Information Systems Security and Privacy Act of 1971" for DOJ in response to the Mathias amendment. This bill essentially would have codified the NCIC privacy and security policies and afforded substantial discretion to the Attorney General with respect to implementation. In 1972, Sen. Hruska introduced a similar bill, except that it provided for reversal of the *Menard v. Mitchell* decision. Both bills were referred to committee with no further action taken.

In 1972 and 1973, Cong. Don Edwards introduced bills to establish privacy and security standards for the dissemination and use of criminal arrest records, and to regulate all State and local as well as Federal criminal justice information systems receiving Federal funds. Both bills were referred to committee and hearings were held,[25] but no further action was taken.

[24]For a detailed discussion, see Marchand, et al., *History and Background Assessment,* op. cit., pp. 192-202, and, more generally, pp. 72-167.

[25]See, for example, U.S. Congress, House Committee on the Judiciary, Subcommittee No. 4, *Security and Privacy of Criminal Arrest Records, Hearings,* 92d Cong., 2d sess., Mar. 16, 22, 23, and Apr. 13 and 26, 1972.

In February 1974, Sen. Hruska introduced S. 2964, "The Criminal Justice Information Systems Act of 1974," on behalf of DOJ, and Sen. Sam Ervin, Jr. introduced S. 2963, "The Criminal Justice Information Control and Protection of Privacy Act of 1974," on behalf of the Subcommittee on Constitutional Rights of the Senate Judiciary Committee. Both bills reflected much of the work of Project SEARCH, the National Advisory Commission on Criminal Justice Standards and Goals, and the NCIC privacy and security policies. However, the Ervin bill took a more restrictive approach that would have limited all record dissemination to conviction information only and severely constrained noncriminal justice access. Also, the Ervin bill would have created a Federal Information Systems Board to be responsible for administration and enforcement, whereas the Hruska bill would have vested such authority in the Attorney General. Extensive hearings were held on both bills.[26] The result was a compromise bill introduced by Sen. Ervin in December 1974. No further action was taken that year.

In 1975, Sen. John Tunney, then Chairman of the Senate Judiciary Subcommittee on Constitutional Rights, and Cong. Don Edwards, Chairman of the House Judiciary Subcommittee on Civil and Constitutional Rights, reintroduced the original 1974 Ervin and Hruska bills and the Ervin compromise bill. Hearings were held in both the House and Senate.[27] Because of continuing disagreements among DOJ, the International Association of Chiefs of Police, Project SEARCH, various State officials (e.g., the Attorney General of Massachusetts), and the American Civil Liberties Union, among others, no further action was taken on these bills or on a new compromise bill introduced by Sen. Tunney.[28]

Since 1975, there have been no new congressional or executive branch initiatives for comprehensive legislation. The proposed FBI Charter legislation did make some limited reference to criminal justice information systems; and Senate Judiciary Committee hearings were held in late 1979 on sections 535(c), 536(d), and 536(e), the provisions of the Senate version (S. 1612) that related to the collection and dissemination of criminal history information. However, FBI Charter legislation was not enacted by the 96th Congress and is not under consideration by the 97th. Also, in 1980 and 1981, the Senate passed amendments to the DOJ Appropriations Authorization Act to mandate a new, comprehensive study of DOJ criminal justice information systems, and to reaffirm the congressional prohibition on message switching unless and until a message switching plan has been approved by the appropriate committees of Congress.[29]

[26] See U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Constitutional Rights, *Criminal Justice Data Banks, Hearings 1974,* vol. I, hearings, vol. II, app., 93d Cong., 2d sess., March 1974.

"see U.S. Congress, Senate Committee on the Judiciary Subcommittee on Constitutional Rights, *Criminal Justice Information and Protection of Privacy Act of 1975,* 94th Cong., 1st sess., July 15 and 16, 1975; and U.S. Congress, House Committee on the Judiciary, Subcommittee on Civil and Constitutional Rights, Criminal *Justice Information Control and Protection of Privacy Act of 1975,* 94th Cong., 1st sess., July 14, 17, and Sept. 5, 1978.

[28] For further discussion of the legislative and policy history, see Marchand, et al., *History and Background Assessment,* op. cit., and also Donald A. Marchand, *The Politics of Privacy, Computers, and Criminal Justice Records,* Information Resources Press, Arlington, Va., 1980.

[29] See S. 2377, sec. 113, 96th Cong., 2d sess.; and H.R. 4169, 97th Cong., 1st sess., and Senate Amendment No. 612 passed by Senate rollcall vote of 85-O on Nov. 12, 1981.