University of Michigan Journal of Law Reform

Volume 7

1974

# Protection of Privacy of Computerized Records in the National Crime Information Center

Stuart R. Hemphill
*University of Michigan Law School*

# PROTECTION OF PRIVACY OF COMPUTERIZED RECORDS IN THE NATIONAL CRIME INFORMATION CENTER

After two New York State troopers stopped an automobile for speeding, a routine inquiry on the vehicle's four occupants was made through a New York State computer facility linked to an FBI computerized criminal information system. The computer's quick response revealed that one of the occupants was wanted by a midwestern police department on a weapons violation. Prompted to investigate further, the troopers found that a woman passenger possessed a revolver, a pistol, a knife, and a small quantity of marijuana. Further search revealed an automatic machine gun with hollow point bullets and three pounds of heroin, valued at $250,000, in the vehicle's trunk. This episode is representative of numerous incidents where the FBI's computerized criminal data system, the National Crime Information Center (NCIC), has provided virtually instantaneous information of unexpected value to a law enforcement agent.[1]

Since the 1920's, the FBI, under authority derived from the Justice Department, has maintained files containing information about individuals and has made most of this information available to authorized agencies and institutions.[2] Over the years the number of records maintained continually increased, as did the number of information requests. This trend, coupled with the increasingly interstate character of crime, forced the FBI to turn from an operation dependent on manual records and mail delivery to a system utilizing the scale and speed of modern data processing equipment. At approximately the same time, automatic information processing technology began to mature.[3] By the 1960's, the computer industry could provide a databank system with centrally stored records that could be accessed directly and swiftly through a network of computer terminals manned by law enforcement agencies throughout the country.

In 1965, plans were announced for an integrated nationwide criminal information network. After extensive testing, a pilot phase NCIC system

[1] This episode appeared in the May, 1973, issue of the NCIC Newsletter, which is published by the FBI and circulated among the state and local agencies participating in the NCIC system. One or two similar episodes appear in each issue of the monthly newsletter under the heading "Hits on the System".

[2] In accordance with 28 U.S.C. § 534(a) (1970), the Attorney General is directed to

> (1) acquire, collect, classify, and preserve identification, criminal identification, crime, and other records; and (2) exchange these records with, and for the official use of, authorized officials of the Federal Government, the States, cities, and penal and other institutions.

Under 28 C.F.R. § 0.85 (1972), the Director of the FBI is authorized to execute these powers under the general supervision and direction of the Attorney General.

[3] An earlier attempt by the FBI to use calculating machines to solve its record-keeping problems proved to be premature. In 1934, a punch-card system for searching fingerprint records was installed, but later abandoned when the volume of prints received grew beyond system capacity. NATIONAL ACADEMY OF SCIENCES, DATABANKS IN A FREE SOCIETY 51 (1972) [hereinafter cited as DATABANKS IN A FREE SOCIETY].

went into operation in January, 1967.[4] Initially, only records of wanted persons and stolen property were maintained. It was stated, however, that additional criminal information might be added as the system took shape.[5] In 1968 and 1969, the stolen property files were expanded, and in November, 1971, a national computerized criminal history (NCCH)[6] file[7] was made operational.[8] The current NCIC system maintains files on wanted persons; stolen vehicles, including aircraft and snowmobiles; license plates, guns, and other identifiable articles; stolen securities; stolen boats; and offenders' criminal histories.[9] As of January, 1972, the system network included terminals in numerous state and local law enforcement agencies and in all FBI field offices, thus allowing on-line access by some 6,000 law enforcement agencies in the United States and Canada.[10]

The purpose of this article is to describe the social benefits and costs of the NCIC and to indicate the need for a program of operational controls to temper the system's impact on the balance between individual privacy and law enforcement needs. Various approaches which could be incorporated into a program of safeguards are introduced and briefly analyzed. Finally, the article discusses several overall design issues which should be considered in the construction of an adequate program of safeguards. Particular emphasis is placed on the NCCH file since it is the major source of the tensions underlying the issues addressed.

## I. SOCIAL BENEFITS AND COSTS OF THE NCIC

### *A. Benefits*

The NCIC, particularly the NCCH file, offers major benefits to several groups. It has proven its usefulness to law enforcement agents by provid-

[4] This pilot phase system linked together fifteen police jurisdictions and included some 23,000 records on file. *Id.* at 52-53.

[5] The statement was made by an FBI spokesman at the opening-day demonstration. *Id.* at 53.

[6] Although the FBI uses the acronym CCH to designate its national computerized criminal history file, the acronym NCCH will be used hereinafter in order to avoid confusion with the standard abbreviation of Commerce Clearing House.

[7] The national criminal history file concept was developed by a project called SEARCH (System for Electronic Analysis and Retrieval of Criminal Histories) initiated by the Law Enforcement Assistance Administration (LEAA) of the Justice Department. Although a representative of the FBI worked with the project during at least part of its early months, eventual FBI control of the criminal history file was not a part of the original plan. Control of the system could have been given to a multistate consortium with one state office serving as a message-switching center. Alternatively, the LEAA might have coordinated the system through a clearinghouse administered by the International Association of Chiefs of Police. Vesting control in the FBI was another possibility. After intense behind-the-scenes lobbying, Attorney Generall Mitchell transferred primary responsibility for managing the proposed system from the LEAA to the FBI. DATABANKS IN A FREE SOCIETY, *supra* note 3, at 57-59.

[8] FBI L. ENFORCEMENT BULL., Jan., 1974, at 8.

[9] *Id.*

[10] FBI L. ENFORCEMENT BULL., Feb., 1972, at 3-4.

ing on-the-spot information concerning objects and persons, thus permitting an investigating officer to exploit an opportunity that he otherwise might not have recognized.[11] The NCIC may also give an officer an idea of the dangerousness of the persons that he is confronting. Information supplied through the NCIC to employers and licensing agencies authorized to receive it[12] undoubtedly speeds their decision-making processes and helps eliminate applicants whose criminal records suggest that they would be particularly unsuited for a sensitive position. The NCIC may also facilitate the operation of the criminal justice system in matters of bail, probation, sentencing, and parole.[13] Although the NCIC's application to these matters appears undocumented, its potential usefulness seems clear, particularly for expediting the bail-setting process. The NCIC is clearly a versatile tool whose benefits are not limited to criminal apprehension.

### *B. Costs*

The detrimental effects of the NCIC mainly result from the greater availability of an individual's criminal record once it is placed in the NCCH file.[14] The group most obviously affected is persons seeking employment or licenses. Records will usually reach employers and licensing boards in a legal manner since both the FBI and the state and local participants in the NCIC may release records to such entities.[15] Unfortunately, experience shows that unauthorized groups also receive criminal records. One inquiry determined that police records were regularly released for preemployment investigations in St. Louis and Baltimore; in New York City, Los Angeles, San Francisco, and Boston, influential employers could obtain records despite contrary policies or regulations.[16] In

---

[11] *See* note 1 and accompanying text *supra*.

[12] State and local agencies participating in the NCIC may provide records to agencies and institutions in accordance with the laws of the state where they are located. *See* DATABANKS IN A FREE SOCIETY, *supra* note 3, at 62; FBI L. ENFORCEMENT BULL., Jan., 1974, at 9. In addition, regulations interpreting 28 U.S.C. § 534(a)(2) (1970), see note 2 *supra*, authorize the FBI to exchange records with railroad police, national banks, member banks of the Federal Reserve System, FDIC-Reserve-Insured Banks, and banking institutions insured by the Federal Savings and Loan Insurance Corporation. 28 C.F.R. § 0.85(b) (1972).

[13] *See, e.g.*, Menard v. Mitchell, 328 F. Supp. 718, 726 (D.D.C. 1971); *Hearings on H.R. 9272 Before a Subcomm. of the Senate Comm. on Appropriations*, 92d Cong., 1st Sess. 212-13 (1971) (statement of FBI Director J. Edgar Hoover); FBI L. ENFORCEMENT BULL., Jan., 1974, at 9. The possibility of developing a nationwide computerized information system for prosecutors which would be linked with the NCIC is mentioned in *Hearings on Street Crime in America (Prosecution and Court Innovations) Before the House Select Comm. on Crime*, 93d Cong., 1st Sess., pt. 3, at 1183-86, 1238 (1973).

[14] This greater availability is also the key to the system's great utility.

[15] *See* note 12 *supra*.

[16] *Hearings on S. 2732 Before the Subcomm. on National Penitentiaries of the Senate Comm. on the Judiciary*, 92d Cong., 2d Sess. 177 (1972) [hereinafter cited as *Hearings on S. 2732*]. Contained in the report of the hearing is the statement of Aryeh Neier and John Shattuck, for the American Civil Liberties Union, referring to the REPORT OF THE COMMITTEE TO INVESTIGATE THE EFFECT OF POLICE ARREST RECORDS

some cases, review of a criminal record is necessary and useful for the protection of the employer's or the public's interest, but in other cases reference to a job or license applicant's record only results in an unnecessary handicap. The relevance of a criminal record varies with the type of job or license being sought and the particular criminal history of the applicant. Where employers and licensing boards err on the conservative side in their decisions, persons with criminal records may be needlessly discriminated against. This discrimination is particularly unfair if the criminal record involves an arrest followed by acquittal or failure to prosecute. In these circumstances, a basic tenet of our criminal justice system asserts that the individual arrested is innocent. Many employers will tend to assume the opposite.[17]

Unnecessary injury to an individual's reputation can also result if criminal records stray from their proper paths. This type of injury could manifest itself in the form of economic detriment or in the more intangible form of social stigma.

The potential for information disclosure may have a "chilling effect" on both the individual and the necessary tensions of the democratic system as a whole.[18] In recent years, the exercise of certain civil liberties has sometimes involved the risk of arrest. Often the arrest is justified, but it may also serve as a tool of harassment. With a national criminal record system, the report of such an arrest may no longer nestle deep in the files of some municipality. The record is far more likely to be stored in the NCCH file, thereby becoming available in almost any jurisdiction in the

---

ON EMPLOYMENT OPPORTUNITIES IN THE DISTRICT OF COLUMBIA (1967). Their statement mentions two other reports documenting loose security, access, and dissemination practices for police files.

Although most of the records systems involved in the documented abusive practices are manual systems, the computerization of records in the NCIC can be expected to increase the potential for unauthorized dissemination and misuse of criminal records. *Id.*; *see* part II *infra*. In Menard v. Mitchell, 328 F. Supp. 718 (D.D.C. 1971), the court considered a suit brought by a man detained as a burgulary suspect in California to recover a record of the detention which had been forwarded to the FBI. The effect of the NCIC on the availability of the record was discussed in plaintiff's brief. After examining the FBI's record-keeping operations the court concluded:

> The Bureau cannot prevent improper dissemination and use of the material it supplies to hundred of local agencies. . . . Control of the data will be made more difficult and opportunities for improper use will increase with the development of centralized state information centers to be linked to the Bureau.
>
> . . . .
>
> In short, with the increasing availability of fingerprints, technological developments, and the enormous increase in population, the system is out of effective control.

*Id.* at 727.

[17] For a full discussion of the loss of employment opportunities due to the existence of a criminal record see *Special Project, The Collateral Consequences of a Criminal Conviction*, 23 VAND. L. REV. 929, 1001-18, 1159-68 (1970). For discussions of such problems in light of a proposed law on nullification of criminal records see *Hearings on S. 2732*, *supra* note 16.

[18] *See generally* A. WESTIN, PRIVACY AND FREEDOM 23-26 (1967). *See also* Menard v. Mitchell, 328 F. Supp. 718, 726 (D.D.C. 1971).

country. The deterrent impact on those facing potential arrest may be marginal, but the balances of a democratic system are often tipped by marginal differences.

Even legitimate use of criminal record information by criminal justice agencies may result in harm to the individuals concerned. Through use of the NCCH file, a judge or other public official could be provided with the full criminal record of an arrested or convicted person where formerly only a partial record from a single state might have been available. This increase in criminal background information is rarely balanced by any increase in information concerning family, employment, psychological history, or other noncriminal circumstances which may be equally critical for proper bail, probation, sentencing, or parole decisions.[19] Thus, in the context of these important decisions, the ready availability of information from the NCIC could tend to produce a one-sided picture of the arrested or convicted individual's background.

It appears that the benefits of the NCIC, although substantial, are purchased at the price of injury to individuals facing unnecessary economic or social harm as a result of the wider availability of their criminal records. Individual injury may result from legitimate as well as illegal use of the system. The threat of such injury may lead to certain inhibiting effects on activities necessary to a democratic system.

## II. THE NCIC AND THE BALANCE OF PRIVACY AND DISCLOSURE

The essential problem presented by the NCIC is best framed as a privacy-disclosure controversy. At the most general level, this controversy is the result of the tension between two reasonable propositions. On the one hand, rational decision-making in a complex and mobile society requires that large amounts of information be widely available. On the other hand, the collection, maintenance, and dissemination of such necessary information interferes with certain psychological and economic prerogatives of the individual, often collectively referred to as "rights of privacy."[20] The privacy-disclosure controversy is not new. Law enforcement officials have kept criminal records for many years. Disclosure of these records has long resulted in similar social and economic detriment.[21] What difference, then, has the presence of the NCIC made? The answer

[19] In at least one major city private groups have attempted to participate in bail hearings to offer family background or employment information for the consideration of the decisionmaker. Chicago Sun-Times, June 2, 1971, at 40, col. 1.

[20] Professor Arthur R. Miller, in a seminal article on computers and privacy, defined the basic attribute of a right of privacy as the individual's ability to control the flow of information which concerns or describes him. Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 MICH. L. REV. 1089, 1107 (1969). Although protection against unsolicited mailed pornography has also been called a privacy right, suggesting that privacy also consists of some control over information flowing to an individual, for purposes of this article Professor Miller's definition remains useful.

[21] *See generally Special Project, supra* note 17.

is found by examining the new factors introduced during the transition from manual record-keeping to a computerized databank, which has made criminal records more widely available and upset the traditional balance between privacy and disclosure.

Four basic factors distinguish the NCIC from previous criminal record systems.

1. *Centralization of Data*—The NCIC is designed to bring together criminal data compiled throughout the entire United States. Part of this centralization is physical: records from many jurisdictions are placed in the storage devices of the central computer facility in Washington, D.C. Part of the centralization is logical: the system ties together data stored in state and metropolitan criminal information systems. All records become part of a nationwide computer and telecommunications network.[22]

2. *Decentralization of Access*—By centralizing records in one computer network, the NCIC makes any record in the system available at any one of the planned 45,000 terminals[23] across the country. Leased communication lines link the existing computers and terminals.

3. *Proliferation of Copies*—The computer, like a photocopy machine, will faithfully produce copies at superhuman speeds. Unlike a photocopy machine, however, the computer can deposit copies at several geographical locations by routing output to any requesting terminal.[24]

4. *Abstraction, Abbreviation, and Standardization of Data*—The structure of computer languages, control programs, and storage devices makes every letter and number in a record important. The result is a record distilled into codes, abbreviations, and terse verbal formulations.[25]

Centralization of data, decentralization of access, and the proliferation of copies all contribute to the great availability of data from the NCIC system. The possibility of illegal access is enhanced since there are many more opportunities for corruption of personnel and since the broad network of communication lines is vulnerable to electronic penetration.[26] Simultaneously, the abstraction, abbreviation, and standardization of data

---

[22] It appears that the original concept of a national criminal history file as proposed by SEARCH (*see* note 7 *supra*) was based on a central index which would coordinate the exchange of records maintained primarily in state computer systems. DATABANKS IN A FREE SOCIETY, *supra* note 3, at 58. Although this is still the ultimate concept for the NCCH file, currently the national "index" file actually contains the complete record for multistate offenders. Indications are that this practice will continue until all states have developed the necessary computer capabilities. FBI L. ENFORCEMENT BULL., Jan., 1974, at 10.

[23] Letter from Francis W. Sargent, Governor of Massachusetts to the Editor of the New York Times. N.Y. Times, Nov. 27, 1973, at 40, col. 4.

[24] For most purposes a computer can treat a printing device located hundreds of miles away in the same way that it treats a device located in the same room. In both cases, the desired message is transmitted via electromagnetic signals over a communications channel.

[25] *See generally* the portion of plaintiff's brief in Menard v. Mitchell, 328 F. Supp. 718 (D.D.C. 1971), which is reprinted in *Hearings on S. 2732, supra* note 16, at 179-81.

[26] Computer communication lines resemble, and often consist of, telephone lines. Thus, they can be "tapped" in much the same manner. *See* A. WESTIN *supra* note 18, at 79-80.

make it more likely that information will be misunderstood, and, in the case of criminal history records, less likely that the record will convey a full and accurate picture of the individual involved. Thus, greater availability makes the label of criminal more inescapable than ever, even for those who have been rehabilitated and seek to lead normal lives.

Where stored data such as the license and serial numbers of stolen property are concerned, the factors outlined above have less significance. While potential inaccuracies and the cryptic quality of computer data continue to be problems, numbers do not undergo abbreviation or abstraction. The greater availability of license and serial number data may affect criminals, but making the criminals' task more difficult or risky cannot be construed as prejudicing their rights.

In addition to the new problems associated with the four factors discussed above, the accuracy and currency problems of manual record-keeping continue under the NCIC. Ironically, in the midst of electronic wizardry, update and correction functions still depend on the skill and energy of human beings. Indeed, accuracy and currency problems in the NCCH file may prove to be aggravated in comparison to the FBI's previous manual system since the state criminal justice agency first entering the record into the file is given the primary responsibility for its updating and modification.[27] Whether accuracy and currency can be maintained in a system with such diffuse responsibility is questionable.

Since computer databanks are widely accepted and their use in an expanding NCIC is likely to continue, the four factors previously mentioned will continue to affect the balance between privacy and disclosure in criminal record-keeping. The next section assesses the capacity of existing statutes, regulations, judicial doctrines, and operational policies to function as preventive and remedial safeguards in redressing the changed balance between privacy and disclosure.

## III. THE INADEQUACY OF CURRENT SAFEGUARDS FOR THE NCIC

The operational balance struck between the protection of individual privacy and the needs of law enforcement in a system like the NCIC will to a great extent be a function of the legal and administrative environment in which it functions. In order to balance effectively the social costs and benefits arising from the greater availability of individual criminal data, there must be legal and administrative safeguards which regulate the availability of records and attempt to blunt the derimental effects of greater availability. The legal and administrative environment in which the NCIC currently operates is derived from three sources: 1) the statutes and regulations on which the NCIC is based; 2) judicially developed doctrines grounded in common law or the Constitution; and 3) the NCIC's

[27] FBI L. ENFORCEMENT BULL., Feb., 1972, at 26.

own informal procedures, guidelines, and customs. A brief review of these sources suggests that current safeguards for the NCIC are inadequate.

In examining a program of safeguards for the NCIC NCCH file it is useful to define four distinct categories of data:

1. *Arrest Records*—records of arrests where no prosecution followed or no conviction resulted from prosecution.
2. *Conviction Records*—records of actual criminal convictions, including guilty pleas and pleas of *nolo contendere;* related records concerning sentencing, parole, and other contacts with the criminal justice system arising from convictions.
3. *Nullified Conviction Records*—records of conviction which have been the subject of a successful expungement proceeding.
4. *Narrative Records*—raw investigative or surveillance data.[28]

Criminal records differ across and within these categories as to the sensitivity of the data contained, their public availability, their accuracy as reports of past criminal activity, and their reliability as predictors of future criminal behavior. These differences mean that the type of preventive and remedial efforts which are necessary, possible, and acceptable will vary according to the kind of record involved. Thus, one measure of the effectiveness of a system of safeguards is whether it responds to differing types of records in an appropriate manner.

### *A. Statutes and Regulations Affecting the NCIC*

The basic statutory authority for the NCIC is a broad information collecting and exchanging mandate given to the Attorney General.[29] The statute dates essentially from 1930.[30] Its language is open-ended both as to the kinds of information which can be collected and maintained[31] and as to the institutions that may participate in the "exchange" of records.[32] Thus, the FBI is authorized to include any type of criminal record in the NCIC and to disseminate any record it maintains to a broad range of

---

[28] Currently, the NCIC's NCCH file contains arrest and conviction records. Narrative records have not been put into the system. A NCIC spokesperson has indicated that the FBI has no present plan to put individual intelligence information into any computerized databank and, in any case, this would not be attempted until the use and protection of this data is better understood. DATABANKS IN A FREE SOCIETY, *supra* note 3, at 63.

Nullified records might exist in the NCCH file since several states provide statutory procedures for the nullification or expungement of criminal records. *See* Comment, *Branded: Arrest Records of the Unconvicted,* 44 MISS. L. J. 928, 931-34 (1973); *Special Project, supra* note 17, at 1149 nn.22-23. Such proceduees usually require the sealing or destruction of all copies of the record nullified. Although the FBI will honor requests to return records, state officials may overlook the existence of the FBI copy.

[29] 28 U.S.C. § 534 (1970). *See* note 2 *supra.*

[30] A ruling secured from the Attorney General declared that the 1930 federal statute was a sufficient legal foundation for the NCIC, thereby making new enabling legislation unnecessary. DATABANKS IN A FREE SOCIETY, *supra* note 3, at 52.

[31] 28 U.S.C. § 534(a)(1) (1970). *See* note 2 *supra.*

[32] *Id.* § 534(a)(2).

governmental and private institutions.[33] The sole statutory sanction for abuse of the information collecting and exchanging functions is directed toward recipient organizations. This provision, which subjects the information exchange "to cancellation if dissemination is made outside the receiving departments or agencies,"[34] has seldom been invoked.[35] Although legislation designed to build additional statutory protections around the operation of criminal justice information systems was proposed as early as September, 1971,[36] the basic statutory authority has not been modified. As a result, the NCIC can maintain and disseminate virtually any type of criminal record with few limitations. Individuals whose records are maintained have no federal statutory remedies tailored to redress abuse of the system, no matter how sensitive the recorded information or how unreliable and prejudicial it is for the purpose for which it was released.

### *B. Judicially Developed Safeguards*

Although judicially developed doctrine provides little that is of direct value as a safeguard for the NCIC, recent cases suggest several positions which the courts may take to protect against unnecessary maintenance and dissemination of criminal records.[37] The traditional judicial refusal to interfere with the handling of criminal data[38] has been abandoned as courts take greater notice of the disabilities resulting from criminal record disclosure.[39] Several courts have attempted to set limits on use and dis-

---

[33] A specific regulation, 28 C.F.R. § 0.85(b) (1972), now limits the class of participants in the exchange. *See also* note 12 *supra*.

[34] 28 U.S.C. § 534(b) (1970).

[35] The FBI has withdrawn dissemination privileges from only six small town police departments in the last ten years, despite "overwhelming evidence" of improper dissemination and unauthorized use of such data in recent years. *Hearings on S. 2732 supra* note 16, at 177 (statement of Aryeh Neier and John Shattuck for the American Civil Liberties Union).

[36] *See, e.g.*, S. 2546, Criminal Justice Information Systems Security and Privacy Act of 1971, 92d Cong., 1st Sess. (1971).

[37] *See, e.g.*, Menard v. Mitchell, 328 F. Supp. 718 (D.D.C. 1971); United States v. Kalish, 271 F. Supp. 968 (D.P.R. 1967); Eddy v. Moore, 5 Wash. App. 334, 487 P.2d 211 (1st Div. 1971). These cases have received attention in several articles and notes. *See, e.g.*, Steele, *A Suggested Legislative Device for Dealing with Abuses of Criminal Records*, 6 U. MICH. J.L. REFORM 32 (1972); Comment, *Branded: Arrest Records of the Unconvicted*, 44 MISS. L. J. 928 (1973); Comment, *Police Records of Arrest: A Brief for the Right to Remove Them from Police Files*, 17 ST. LOUIS U.L.J. 263 (1972); Comment, *Maintenance and Dissemination of Criminal Records: A Legislative Proposal*, 19 U.C.L.A.L. REV. 654 (1972); Comment, *Retention and Dissemination of Arrest Records: Judicial Response*, 38 U. CHI. L. REV. 850 (1971).

[38] Comment, *Retention and Dissemination of Arrest Records: Judicial Response*, 38 U. CHI. L. REV. 850, 854 (1971). *See* cases collected *id.* at 854 n.20.

[39] *See, e.g.*, Menard v. Mitchell, 430 F.2d 486, 490-91 (D.C. Cir. 1970); Morrow v. District of Columbia, 417 F.2d 728, 741-43 (1969); Henry v. Looney, 65 Misc. 2d 759, 762, 317 N.Y.S.2d 848, 851 (Sup. Ct. 1971).

The *Menard* court made the following finding:

> Information denominated a record of arrest, if it becomes known,

tribution of arrest records by law enforcement agencies.[40] Although there appear to be no cases supporting judicial controls on the retention and distribution of conviction records by law enforcement groups, one court has moved to prevent disclosure made by private organizations.[41]

A tort privacy theory is the only well-developed judicial doctrine currently available to courts for use in cases involving injury from the disclosure of criminal records.[42] However, this theory excludes a number of injurious disclosure situations where protection would be desirable.[43] While a constitutional privacy doctrine appeared as an explicit ground of decision in at least one case involving criminal records,[44] it is probably not a reliable legal theory for ensuring the protection of specific privacy rights not yet firmly recognized.[45]

Most courts treat the problem of maintenance and disclosure of criminal records as one of balancing[46] the individual's interest in nondisclosure against the public interest in the ready availability of criminal records as

---

> may subject an individual to serious difficulties. Even if no direct economic loss is involved, the injury to an individual's reputation may be substantial. Economic losses themselves may be both direct and serious.

Menard v. Mitchell, 430 F.2d 486, 490 (1970). The cases cited above all dealt with arrest records. The catalogue of disabilities would be still more extensive for conviction records.

[40] *See, e.g.*, Menard v. Mitchell, 328 F. Supp. 718 (D.D.C. 1971); Eddy v. Moore, 5 Wash. App. 334, 487 P.2d 211 (1st Div. 1971). The *Menard* court construed the FBI's statutory authority (*see* notes 23-25 and accompanying text *supra*) narrowly to find that the Bureau was "without authority to disseminate arrest records outside the Federal Government for employment, licensing or related purposes whether or not the record reflects a later conviction." 328 F. Supp. at 727. A rider to a bill passed several months after this decision restored the authority of the FBI to its previous status for a period of one year. DATABANKS IN A FREE SOCIETY, *supra* note 3, at 61.

[41] *See, e.g.*, Briscoe v. Readers' Digest Ass'n, 4 Cal. 3d 529, 483 P.2d 34, 93 Cal. Rptr. 866 (1971).

[42] *See* W. PROSSER, LAW OF TORTS § 117 (4th ed. 1971). Of the four distinct types of privacy invasion discussed, the action based on public disclosure of private facts appears to have the greatest conceptual congruence with an action based on disclosure of criminal records. The elements of this disclosure tort are: 1) that the facts disclosed be private facts not public ones; 2) that the disclosure be public not private; and 3) that the matter disclosed be one which would be offensive and objectionable to a reasonable man of ordinary sensibilities. *Id.* at 810-11. The "false light" or defamation type privacy action may also be useful to a plaintiff who has been harmed by publication of his record. *See generally* Comment, *supra* note 38, at 868-69.

[43] Comment, *supra* note 38, at 869; Comment, *Maintenance and Dissemination of Criminal Records: A Legislative Proposal*, 19 U.C.L.A.L. REV. 654, 655-56 (1972). For example, disclosure to an employer might not be "public disclosure" sufficient to support an action. Disclosure of a conviction which is a matter of public record may fail to satisfy the requirement for disclosure of a private fact.

[44] Eddy v. Moore, 5 Wash. App. 334, 487 P.2d 211 (1st Div. 1971).

[45] In the following cases, specific constitutional rights of privacy were found: Berger v. New York, 388 U.S. 41 (1967) (against eavesdropping); Griswold v. Connecticut, 381 U.S. 479 (1965) (against invasion of marital privacy); Townsend v. Sain, 372 U.S. 293 (1963) (against compelled submission to truth drugs); Mapp v. Ohio, 367 U.S. 643 (1961) (against unrestrained search and seizure); Nardone v. United States, 308 U.S. 338 (1939) (against surreptitious wiretapping).

[46] *See, e.g.*, cases cited in note 37 *supra*.

an aid to law enforcement.[47] Although the balancing approach is flexible and offers no theoretical barriers to further judicial development of safeguards against abuses of criminal records, its flexibility will mean delay and uncertainty until the doctrines mature. Judicial doctrines, in their current posture, show potential as a partial solution for the problems of maintenance and dissemination of arrest records, but they fail to deal adequately with other types of criminal records or with the damage that can result from abusive dissemination.

### *C. The NCIC's Informal Safeguards*

While it is difficult to tell exactly what sort of informal safeguards the FBI has imposed on the operations of the NCIC, it appears that an initial reluctance[48] to accept a system of safeguards has faded.[49] A Security and Confidentiality Committee created by the NCIC's Advisory Policy Group has developed a set of recommendations which draws heavily on the extensive security and privacy policy recommendations of Project SEARCH.[50] These recommendations include limitations on the type of records maintained; records of minor violations (*e.g.*, drunkenness and vagrancy) and juvenile offenses would be excluded. The Advisory Policy Group further proposed that records be removed in accordance with the state or federal law binding the agency submitting the record. The quality of the data maintained would be assured by certain practices relating to accuracy including the use of system audits. Separation of the criminal record databank from other databanks containing noncriminal information

---

[47] The concerns of law enforcement agencies and the individual interest in privacy may not always be the only factors which should influence the balancing process. Other interests supporting disclosure in a given case relate to freedom of the press and the value of an informed public. Somewhat less compelling concerns are those of commercial operations seeking to avoid the risks incurred through hiring or dealing with individuals possessing criminal records. These other interests will, in most cases, be insignificant when compared with the interests of the individual and the criminal justice system.

[48] Evidence of this initial reluctance appears in a letter from Jerome J. Daunt of the NCIC to O. J. Hawkins of the California Department of Justice, reprinted in *Hearings on Federal Data Banks, Computers and the Bill of Rights Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 92d Cong., 1st Sess., pt. 1, at 1026-27 (1971) [hereinafter cited as *Hearings on Federal Data Banks*]. Mr. Daunt's letter expressed general disapproval of the broad scope of the interim report of the SEARCH Security and Privacy Committee. Specifically, he felt that the report should not speak of an absolute right to privacy. Rather it should confine itself to existing judicial decisions and not speculate on what courts might say in the future. Mr. Daunt also felt that the report expressed a distrust of the entire criminal justice system and that further studies of the privacy-security matter could be deferred.

[49] The FBI's more recent attitude is evinced by a statement that "[t]he FBI also encourages the enactment of Federal legislation which the Congress may deem appropriate to the preservation of rights of the individual and of our society." FBI L. ENFORCEMENT BULL., Jan., 1974, at 10.

[50] DATABANKS IN A FREE SOCIETY, *supra* note 3, at 61. For information on SEARCH see note 7 *supra*.

and the imposition of physical, personnel, and technical security measures would enhance the integrity of the system. Dissemination would be limited by ensuring that all NCIC users are criminal justice agencies. Furthermore, under the Group's recommendations the individual would be given the right to see and challenge the contents of his record.[51] This extensive program was "endorsed" in June, 1971, by former FBI Director Hoover.[52] Currently, state and local participants in the NCIC are required to sign a contract with the director of the FBI, agreeing to abide by this set of safeguards and any future ones.[53] If, as a practical matter, such a program were fully operational within the FBI and each of the state and local participants, it would be a major step toward protection of individuals whose records are kept in the NCCH file.

In light of the preceding discussion, there exist serious doubts about the adequacy of legal and administrative safeguards for the NCIC.[54] Neither the statutory basis of the NCIC nor existing judicially developed doctrines provide sufficient limitations on the maintenance and dissemination of various types of records or effective remedies for abusive disclosure. While the informal system of safeguards endorsed by the FBI does show a broad awareness of the security and privacy problems presented by the NCIC, it can not be truly adequate until it is given greater visibility and enforceability as a program of legislation and administrative regulations.

## IV. Design of a Comprehensive Safeguard Program for the NCIC

The increased potential for damage[55] because of the greater availability of criminal data stored in the NCIC's NCCH file,[56] coupled with the general lack of effective legal and administrative safeguards for the system,[57] make it clear that a scheme of regulations and remedies must be developed. The duty to design and implement effective protective and remedial measures falls on legislators and the administrators of the NCIC.[58] The following discussion surveys some of the more important factors to be considered in system design.

There are various approaches to the implementation of safeguards for criminal record information systems such as the NCIC's NCCH file. Although some of the proposals discussed below were advanced as general

---

[51] DATABANKS IN A FREE SOCIETY, *supra* note 3, at 62.

[52] *Id.*

[53] U.S. DEP'T OF HEALTH, EDUCATION & WELFARE, RECORDS COMPUTERS AND THE RIGHTS OF CITIZENS 233 (1973).

[54] For a somewhat more emphatic statement of the same conclusion see that portion of the opinion of the *Menard* court quoted in note 16 *supra*.

[55] *See* part I *B supra*.

[56] *See* part II *supra*.

[57] *See* part III *supra*.

[58] After cataloging the faults of the FBI's criminal record-keeping activities, the *Menard* court reached the conclusion that "[t]he Bureau needs legislative guidance and there must be a national policy developed in this area which will have built into it adequate sanctions and administrative safeguards." 328 F. Supp. 718, 726-27 (1971).

protective remedies without specific reference to computerized databanks, others were clearly inspired by the existence of the NCIC's NCCH file. It is suggested, however, that the increased interest in safeguards for criminal records is in part a response to the presence of computerized databanks, even in the case of proposals which do not specifically acknowledge the new technology.

Approaches to the problems of providing safeguards can be divided into two types. The first approach includes safeguards directed at the functions of the computerized databank itself—the collection, maintenance and dissemination of criminal data. Included are controls on databank content, which would limit the acquisition and maintenance of certain types of data,[59] ensure that data maintained are current and accurate,[60] and provide for the nullification or expungement of certain kinds of records.[61] Other approaches of this type are aimed at the way data flow from the system. These approaches include procedures and penalties limiting dissemination[62] and deterring physical or electronic penetration of the system. The second type of safeguard does not focus directly on the procedures of data acquisition, maintenance, and dissemination, but rather on external means of reducing the damage done by a given pattern of systemic operation. Included in this category are attempts to control review of criminal data in making certain decisions where its consideration may be unnecessarily prejudicial.[63] Additional procedures of this type would give an individual some knowledge of and control over records concerning him or her.[64] A full program of safeguards must be constructed from elements taken from several of these approaches.

### *A. Specific Approaches*

*1. Provisions Affecting Data Content*—Limits on the type of data which may be acquired can prevent many problems from ever arising, but such limits would be difficult to impose on any system under the control of the FBI because of its broad information-collecting authority.[65] This broad mandate makes expansion of the kinds of data computerized

[59] *See, e.g.*, S. 2697, 93rd Cong., 1st Sess., § 534(c)(1) (1973); H.R. 188, 93rd Cong., 1st Sess., § 3102(d) (1973); H.R. 9783, 93d Cong., 1st Sess., §§ 2(a), (d), (e) (1973); Comment, *Maintenance and Dissemination of Criminal Records: A Legislative Proposal*, 19 U.C.L.A.L. REV. 654, 681-82 (1972.

[60] *See, e.g.*, H.R. 9783, 93d Cong., 1st Sess., §§ 2(b), (c) (1973).

[61] *See, e.g.*, S. 2697, 93d Cong., 1st Sess., § 534(c)(1) (1973) S. 2732, 92d Cong., 1st Sess., §§ 3, 4, 5, 11 (1971); Steele, *supra* note 37, at 50-53.

[62] *See, e.g.*, H.R. 11483, 93d Cong., 1st Sess., §§ 534 (b), (c) (1973); S. 2697, 93d Cong., 1st Sess., §§ 534(d), (f) (1973); H.R. 188, 93d Cong., 1st Sess., §§ 3101, 3102, 3105 (1973); H.R. 9783, 93d Cong., 1st Sess., § 3 (1973); S. 2732, 92d Cong., 1st Sess., § 7(a)(1) (1971); Comment, *supra* note 59, at 679-86.

[63] *See, e.g.*, H.R. 188, 93d Cong., 1st Sess., § 3106 (1973); S. 2732, 82d Cong., 1st Sess., §§ 7(a)(3), 7(b) (1971); Steele, *supra* note 37, at 54-56.

[64] *See, e.g.*, H.R. 188, 93d Cong., 1st Sess., § 3103 (1973); H.R. 9783, 93d Cong., 1st Sess., § 4 (1973); Comment, *supra* note 59, at 686-87.

[65] *See* note 31 and accompanying text *supra*.

both convenient and economical, since both the data and the skills and facilities for its collection and maintenance are already within one organization. Should the FBI choose to computerize its narrative files,[66] for example, it could utilize existing NCIC databank facilities. Assuming that control over the kinds of data computerized is desirable, one solution is to set up an independent agency to administer the databank. The agency's collection and maintenance of records could be conveniently limited through separate statutory or regulatory authorization. If the NCIC remains under the FBI, its independent operation[67] should be ensured and its authority to acquire and maintain records should be separately defined. Until better security facilities and procedures are available, the agency's authority should not include the acquisition and maintenance of narrative records[68] or other data which are highly sensitive or whose accuracy is in doubt. Other restrictions forbidding the acquisition and retention of certain types of arrest records,[69] specific kinds of conviction data,[70] and all nullified and expunged records[71] have also been proposed.

Procedures ensuring the accuracy and currency of records are essential. A provision imposing such a duty,[72] however, could prove to have little more than cosmetic value unless specific measures designed to promote it are articulated and applied.[73] Means of determining which records are inaccurate or out-of-date must be provided together with time limits for entering corrections and updates after notification of error or change of status.[74] An audit by an independent group[75] could provide the necessary checking mechanism and would probably be more effective than allowing an individual to check his own record.[76] But auditing by an inde-

---

[66] *See* note 28 *supra*.

[67] *See, e.g.*, H.R. 9783, 93d Cong., 1st Sess., § 5 (1973), which provides that "Each criminal data bank shall be independent and distinct from any other data collection or storage operation."

[68] *See* note 28 *supra*.

[69] *See, e.g.*, H.R. 188, 93d Cong., 1st Sess., § 3102(d) (1973) (excluding arrest records more than two years old for which there is no prosecution pending and arrest records for which the responsible prosecuting attorney feels no prosecution is warranted); H.R. 9783, 93d Cong., 1st Sess., § 2(a) (1973) (excluding arrest records which are at least two years old if no other arrest appears within the two intervening years).

[70] *See, e.g.*, H.R. 9783, 93d Cong., 1st Sess., § 2(c) (1973) (excluding conviction records more than ten years old, if the intervening ten years have been conviction-free. Juvenile records and records of any offense for which the maximum penalty is less than six months imprisonment or a fine of not more than one hundred dollars are also excluded.).

[71] *See, e.g.*, H.R. 188, 93d Cong., 1st Sess., § 3102(d) (1973) (excluding records which are expunged under a provision of state law).

[72] *See, e.g.*, H.R. 9783, 93d Cong., 1st Sess., § 2(b) (1973) (providing for "periodic updating" and for making additions, corrections, or deletions within ninety days of the receipt of new information).

[73] *See, e.g.*, H.R. 9783, 93d Cong., 1st Sess., § 2(b) (1973) (providing for a systematic outside audit for accuracy). *See also* text accompanying notes 101-02 *infra*.

[74] *See* note 72 *supra*.

[75] *See* note 73 *supra*.

[76] *See, e.g.*, H.R. 9783, 93d Cong., 1st Sess., § 4(a) (1973). Although an individual who understood an auditing program and was aware of the items in his criminal

pendent group could present an additional security risk, since the auditors would be privy to all information in the files.

Additional verification measures, providing incentives to each of the various agencies responsible for maintaining the records,[77] could be built into the computer programs which interact with the files. The computer, with its tireless and virtually boundless memory, is ideally suited both to provide reminders that certain records need further attention and to purge from the active files any obsolete or inaccurate records.[78] A computer is most effective in detecting certain types of formal errors such as omissions or the use of a symbol or abbreviation that it does not recognize. If a record conforms to the prescribed format, however, content errors can be detected only by comparison with an independent source of accurate information. As a result, an effective program for monitoring the accuracy and currency of the information would probably have to include manual and automatic auditing.

Procedures for the expungement or nullification[79] of certain kinds of criminal records are an attractive solution because they appeal to the notion that an individual should be given a chance to clean his slate and make a fresh start. But the formulation and implementation of such procedures present certain problems. First, the proper criteria for nullification are not easy to define and agree on.[80] Second, the structure of the NCIC system encourages the proliferation and broad dissemination of record copies.[81] If nullification is to be truly effective, all copies of the record to be nullified must be located and destroyed or collected and sealed. Legislation setting up nullification procedures would have to be supplemented by a system of accountability[82] for copies. Nullification procedures would

---

record might be more scrupulous in verifying the accuracy of his record than official auditors, this type of awareness and understanding could probably not be found in a criminal population characterized by poor education and mistrust of official processes. However, allowing for a personal audit of an indvidual's record may have an additional value beyond its function in an accuracy program, because of the psychological reassurance and sense of control which it gives the individual. *See* text accompanying notes 101-02 *infra*.

[77] *See* text accompanying note 27 *supra*.

[78] One such measure is already in effect. A programming feature for the file of stolen vehicle records purges any records which have been in the file for more than ninety days without having the vehicle identification number filled in. NCIC Newsletter, Apr., 1973.

[79] Expungement and nullification both refer to the procedure whereby a criminal record is removed from the normal pattern of maintenance and dissemination. Since a major bill on the subject (S. 2732, Offender Rehabilitation Act, 92d Cong., 1st Sess. (1971)) refers to the procedure as nullification, that terminology is used herein. Nullification procedures usually consist of the removal of records from files accompanied by their destruction or return to the person involved or the sealing and segregation of the record.

[80] *See generally Hearings on S. 2732, supra* note 16; *Hearings on Federal Data Banks, supra* note 48, at 856-57.

[81] *See* part II *B supra*.

[82] In the July, 1973, issue of the NCIC Newsletter an item appeared referring to the increasing state use of nullification procedures and the concomitant need to "establish appropriate procedures to maintain accountability for the receipt/destruc-

reincorporate into criminal record systems some of the forgiving and forgetting which allowed deserving individuals to escape or live down their criminal record under local manual record systems. If nullification criteria were properly selected, this procedure could distinguish between records which need to be kept and those which can be discarded, and would accomplish this result more efficiently than the somewhat random process of human memory.

*2. Provisions Affecting Movement of Data*—Procedures and penalties designed to deter physical and electronic penetration of the NCIC computer system and communication network are a necessary part of any adequate program of safeguards. The most appropriate topics for legislation in this area are provisions defining offenses, specifying penalties for "data snooping," and articulating the duty to provide reasonable security measures.

Legislation controlling dissemination of data is the key part of any safeguard program since, despite occasional leaks from the system, the vast majority of the data circulated will reach and remain at its destination under the authority of the system's rules on dissemination. Further, if there are no limits on the types of data that can be collected and mainained,[83] no programs for ensuring accuracy and currency of records,[84] and no procedures for nullification,[85] effective protection can still be realized through utilization of strict rules limiting dissemination. In fact, the rules on dissemination should be a function of the adequacy of measures provided under other approaches. Thus, a limit on dissemination can compensate for a liberal policy on data collection while preserving access to the records for criminal justice agencies.[86] Limitations on the dissemination of records whose acquisition and maintenance are already forbidden are not totally redundant. When criminal actions or civil suits for data abuse are brought, the disseminator may be a more available defendant than the person responsible for maintenance and acquisition of the record that found its way into the wrong hands.

The basic problem in designing controls for dissemination is to match classes of data with groups that have a legitimate need or interest in them. To solve this problem, it may be necessary to refine the categories of records outlined previously[87] into smaller units which fit the narrow needs of or are best suited to the predictable attitudes of the groups that

---

tion/dissemination of CCH records". The item was first published in the January, 1972, Newsletter and republished "because of its continuing importance in maintaining system security." For a provision setting up a system of accountability see H.R. 9783, 93d Cong., 1st Sess., § 2(f) (1973).

[83] *See* notes 69-71 and accompanying text *supra.*

[84] *See* notes 72-78 and accompanying text *supra.*

[85] *See* notes 80-82 and accompanying text *supra.*

[86] For example, if a high value is placed on making arrest records or older, nullified records available to criminal justice agencies, system policy might allow such records to be maintained and disseminated to law enforcement agencies, but not to employers and licensing boards.

[87] *See* note 28 and accompanying text *supra.*

desire access to the data. For example, while a law enforcement agency might be authorized to receive a full arrest record, including arrests not followed by convictions, an employer bank might be entitled to see only arrest data which are less than one year old.[88] It may also be useful to provide for dissemination of processed versions of data to particular groups that have a legitimate use for information but should not see it in its original form. For example, research groups or special task forces may need data that could be provided in edited form without loss of usefulness. The editing process would remove individual names and aggregate records[89] so that no single individual, or even some particularly sensitive group, is identifiable.[90] Provisions for the release of certain kinds of data to the news media may also be appropriate.[91]

Legal remedies for incidents of abuse must be established if any dissemination controls are to be effective. Both criminal penalties[92] and civil causes of action[93] should be provided. In addition, sanctions affecting offending organizations[94] can supplement the deterrent effect of the sanctions against individuals.

*3. Provisions Affecting Utilization of Data*—Controls on the utilization of criminal data in making critical decisions where its consideration might cause unnecessary prejudice can provide an additional level of protection. Direct restrictions on the consideration of a criminal record and the rejection of an applicant because of his criminal record could be applied to many employers and licensing boards.[95] Applicants confronting employ-

---

[88] Other distinctions between records have been suggested. In *Menard v. Mitchell* the court of appeals found that an expungement remedy for arrest records might depend on whether or not the arrest was based on probable cause. 430 F.2d 486, 491-92 (D.C. Cir. 1970). On remand the district court found, however, that "the question of probable cause has little to do with the merits of the underlying controversy." 328 F. Supp. 718, 724 (D.D.C. 1971).

[89] One of the great advantages of computerized databanks for researchers is the speed at which an edited version of the data can be made available by running programs which strip off and reorganize various data items so that the data becomes not only more usable, but less likely to permit the identification of any single individual.

[90] *See, e.g.*, H.R. 9783, 93d Cong., 1st Sess., § 3(f) (1973). The bill provides that "Data may be disseminated by a criminal data bank for the purpose of research, but no data so disseminated shall be identifiable to any person."

[91] *See, e.g.*, the provision suggested in Comment, *supra* note 59, at 684-85.

[92] *See, e.g.*, H.R. 188, 93d Cong., 1st Sess., § 3107(b) (1973) (fine of not more than $1000, imprisonment for not more than one year, or both); H.R. 9783, 93d Cong., 1st Sess., § 6(a)(1) (1973) (fine of $5000 and imprisonment for not more than five years).

[93] *See, e.g.*, H.R. 188, 93d Cong., 1st Sess., § 3107(a) (1973) (action for actual damages, reasonable attorney's fees and other litigation costs authorized); H.R. 9783, 83d Cong., 1st Sess., § 6(a)(2) (1973) (actions for injunctive and declaratory relief against the United States or the responsible official and for actual and punitive damages with a minimum of $1000 per violation).

[94] *See, e.g.*, H.R. 9783, 93d Cong., 1st Sess., § 6(b) (1973) (providing for termination of federal financial assistance to the databank guilty of a violation and for cutting off the offending databank from the exchange of information).

[95] *See, e.g.*, Steele, *supra* note 37, at 54-55 (excluding from consideration in licensing applications any criminal record which has been excluded from maintenance in official state criminal files, and forbidding the rejection of an applicant on the basis

ers or boards who inquire about criminal records can be given the right to deny the existence of arrest[96] and nullified conviction records.[97] The difficulty of actually examining the decision process of an employer or a licensing board makes enforcement of such restrictions problematic, but the problems are comparable to those arising under race, sex, or age discrimination statutes.

While in most contexts the goal is to prevent consideration of criminal data, in some situations where the data must be examined, a statute or regulation requiring consideration of countervailing data provides a partial remedy. For example, consideration of available family, employment, or psychological data in bail, probation, sentencing, or parole decisions might offset the effect of full criminal record availability. As in the case of restrictions placed on employer and licensing board consideration of criminal data, this type of rule attempts to reach a mental process and is difficult to enforce. Nevertheless, it might increase decisionmakers' awareness of the built-in bias of our current databanks, which immortalize the evil that men do.

*4. Provisions for Individual Control and Notice*—Proposed procedures designed to give an individual a certain measure of control over his record are generally based on four elements: 1) the individual's right to see his own record;[98] 2) the right to view a listing of organizations which have requested and received his record;[99] 3) the right to receive notice of any request for or incident of dissemination of his record;[100] and 4) the right to challenge errors in his record and to have them corrected.[101] The first three provisions can do little more than tell the individual who knows what about his criminal past. Assuming that the record was correct when disseminated, any damage resulting from these prior disclosures will probably be beyond remedy. The fourth provision not only gives the person a direct opportunity to ensure that his record is correct and up-to-date, but it also places useful pressure on the responsible agency to keep the record accurate and current. This approach, then, can reduce an individual's fears by keeping him informed of his status and enhance the effectiveness of any program for maintaining accuracy and currency of

---

of a record which is maintained, but which contains no arrest or conviction constituting a bona fide occupational disqualification for the type and character of work under consideration).

[96] *See, e.g.*, H.R. 188, 93d Cong., 1st Sess., § 3106 (1973) (permitting a person questioned about his arrest record to consider the question as referring only to arrest records which a databank may lawfully disseminate, maintain, or use).

[97] *See, e.g.*, H.R. 2732, 92d Cong., 1st Sess., § 7(b) (1971) (providing that the occurrence of events leading to a criminal record item may be denied when that item has been nullified); Steele, *supra* note 37, at 56.

[98] *See, e.g.*, H.R. 188, 93d Cong., 1st Sess., § 3103 (1973); H.R. 9783, 93d Cong., 1st Sess., § 4(a) (1973); Comment, *supra* note 59, at 686-88.

[99] *See, e.g.*, H.R. 188, 93d Cong., 1st Sess., § 3103 (1973); Comment, *supra* note 59, at 686.

[100] *See, e.g.*, Comment, *supra* note 59, at 686.

[101] *See, e.g.*, H.R. 188, 93d Cong., 1st Sess., § 3104 (1973); H.R. 9783, 93d Cong., 1st Sess., § 4(a) (1973).

records. The main disadvantages of this approach are the costs of maintaining the bureaucracy to support these rights and the potential for abuse if effective identification procedures are not used when persons request record review. The provision for notice of requests for and incidents of dissemination could impose a burden on both the NCIC and the individual involved if a particular record were widely disseminated.

### *B. Overall Design Issues*

There are three overall design considerations which should be incorporated into any comprehensive system of safeguards for the NCIC. First, the effectiveness of the safeguards will depend on which provisions are embodied in law and which take the form of administrative regulations or informal system procedures and guidelines. Legal provisions are more visible and enforceable, while administrative procedures offer greater flexibility. Provisions defining civil remedies and criminal penalties and articulating duties to promote data accuracy and system security must have statutorily conferred enforceability. Provisions establishing individual rights or delineating significant limitations on the system should also have statutory status since they can provide public reassurance. On the other hand, provisions likely to be directly dependent on particular computer programs and hardward require the more flexible form of regulations or guidelines, since no computer system is immune to technical evolution and lawmaking seldom keeps abreast of technology. Provisions detailing specific measures against physical or electronic penetration of the NCIC computer network and specifying the verification and purging functions of the computer are more appropriate for informal administrative treatment.

The second overall design issue concerns the binding scope of the safeguards. Although the NCIC was conceived as a cooperative venture between the FBI and state law enforcement agencies, the label of cooperation cannot conceal the fact that delicate problems of federalism are involved.[102] To be truly effective, a program of safeguards would have to apply uniformly to the FBI and all state participants. But agreement on important policy issues such as limits on dissemination and criteria for nullification may not be easy to reach.[103] Without uniform policies in

---

[102] For an expression of concern over problems of this type see Letter from the Illinois Law Enforcement Commission to Attorney General Mitchell, Oct. 15, 1970, reprinted in *Hearings on Federal Data Banks*, *supra* note 48, at 1025-26.

[103] An incident providing evidence of the necessity for a uniform nationwide program of safeguards for information in the NCIC and the difficulty of agreeing on such a program was sparked by Massachusetts' refusal, in June, 1973, to join the NCIC. Massachusetts felt that the safeguards of other participating criminal records systems were insufficient and that NCIC participation would subvert the measures which Massachusetts enforced in its own system for the protection of her citizens. Massachusetts' refusal to join was met by a Justice Department suit aimed at opening Massachusetts' files to the Justice Department or any other federal agency. Attorney General Richardson later ordered the suit dropped. Massachusetts has condi-

these crucial areas, the degree of protection afforded an individual would depend upon the policies of the state from which his record originates or the state from which the request is made. Proposed legislation suggests that Congress expects to be able to exert its legislative power only over agencies of the federal government and federally funded state agencies.[104] It would be unfortunate if limitations on federal power prevented the development of an adequate, uniform set of safeguards for the NCIC.

The third overall design issue focuses on the integration of the various approaches outlined above. The purpose of promulgating an adequate system of safeguards for the NCIC is to establish a working balance between privacy and disclosure. The balance struck must assure that accurate criminal data are readily available to law enforcement groups and a limited number of other institutions having a true need for it, while ensuring that no unnecessary disclosure prejudicial to individual privacy occurs. To accomplish this task, the designer of a system of safeguards must be aware of the effects of each protective measure on this primary objective. Furthermore, he must realize that a combination of approaches can produce effective results. For example, a system governed by strict limits on dissemination and a comprehensive expungement plan, combined with a broad acquisition and maintenance mandate, might offer the same protection as a system combining restricted acquisition and maintenance with liberal dissemination and limited nullification. The advantage of the former system is that it allows maximum availability of information to a limited number of participants having the greatest need for access. The designer must be aware that while a basic decision sharply limiting the types of data which can be maintained affords maximum protection to individuals whose records are excluded, it also deprives law enforcement agencies and other participants of potentially useful information. Since a composite system of safeguards can be designed by incorporating elements from several approaches, the selection of these elements should be governed by their interdependence and the unique values which they promote.

## V. CONCLUSION

When viewed from a neutral perspective, the NCIC is simply a means for facilitating the aggregation and distribution of useful information. NCIC's distinctiveness lies in its ability to fulfill this function on a national scale and to distribute the desired information to the point of request within seconds. From this perspective, the NCIC must be viewed not only as a means of spreading criminal information across the country,

---

tioned its participation in the NCIC on the institution of federal safeguards equivalent to its own. Letter from Francis W. Sargent, Governor of Massachusetts to the Editor of the New York Times. N.Y. Times, Nov. 27, 1973, at 40, col. 4.

[104] *See, e.g.*, H.R. 188, 93d Cong., 1st Sess. (1973), which is aimed at officers or employees of the United States or of a federally assisted law enforcement agency and H.R. 9783, 93d Cong., 1st Sess. (1973), which applies to criminal databanks established and supported by the United States.

but also as an opportunity for fine-tuning the flow of criminal justice information to institutions which can use it effectively and judiciously. This new opportunity carries with it the responsibility for answering many questions about the proper use of the system. By enabling desired criminal data to be widely available, the NCIC forces consideration of the issue of who should have access to what data. The boundaries of time, distance, and cost, which previously determined the answer, no longer function as such rigid constraints. The resolution of this issue is far from easy because the underlying decisions involve uncharted areas of law, psychology, and politics. The necessary and proper boundaries of individual privacy are extremely elusive. The value of criminal data in predicting future antisocial behavior is unclear. The lack of clear answers, however, should not lead decisionmakers to permit policy to be shaped solely by new technology. The premises underlying the still vague notions of privacy should be weighed against the justifications for increasing data collection and disclosure accompanying the rise of databanks.

The appropriate means of controlling the operation of the NCIC is a program of legislative and administrative safeguards. Not only are current safeguards inadequate, but the broad range of controls necessary for an effective program makes timely development of appropriate judicial doctrines unlikely. The recent announcement of legislative proposals for the regulation of law enforcement databanks[105] suggests that this problem is beginning to receive the attention it deserves.

—*Stuart R. Hemphill*

[105] N.Y. Times, Feb. 3, 1974, at 1, col. 8.