Volume 22 | Issue 6 Article 6

1976

Privacy: A Case for Accurate and Complete Criminal History Records

Thomas J. Madden

Helen S. Lessin

PRIVACY: A CASE FOR ACCURATE AND COMPLETE CRIMINAL HISTORY RECORDS

THOMAS J. MADDEN† AND HELEN S. LESSIN††

The President's Crime Commission in its 1967 report entitled *The Challenge of Crime in a Free Society* stated that "[a]n integrated national information system is needed to serve the combined needs at the National, State, regional and metropolitan or county levels of the police, courts, and correction agencies, and of the public and the research community."[1]

At that time only ten states in the nation had automated state level criminal justice information systems.[2] By 1976 almost all of the states had automated information systems in operation. These systems contain the criminal history records of millions of individuals.[3]

This information explosion with its greater capacity to gather, store, process, and transmit criminal justice information has serious consequences for those who come into contact with the criminal justice system. The consequences are particularly severe for the individual who is arrested and who is not subsequently convicted. As one judge noted in a leading case:

> Information denominated a record of arrest, if it becomes known, 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. Opportunities for schooling, employment, or professional licenses may be restricted or nonexistent as a consequence of the mere fact of an arrest, even if followed

† Assistant Administrator/General Counsel, Law Enforcement Assistance Administration, United States Department of Justice. B.E.E., Villanova University, 1964; J.D., Columbus School of Law, Catholic University, 1968.

†† Attorney-Advisor, Law Enforcement Assistance Administration, United States Department of Justice. B.A., Queens College, 1958; J.D., Washington College of Law, American University, 1971.

1. Report by the President's Comm. on Law Enforcement and Admin. of Justice 267 (1967) (Sup. Doc. No. PR 36.8:L41/C86).

2. Law Enforcement Assistance Administration, 1972 Directory of Automated Criminal Justice Information Systems (Sup. Doc. No. J1.8/2:Au8/972).

3. The number of current criminal history records maintained in the United States at the state and local level is approximately 195 million. *See The American Criminal History Record Present Status and Future Requirements,* Technical Report No. 14, SEARCH Group, Inc., Sacramento, Cal. (1976) [hereinafter cited as Technical Rep. No. 14]. This number includes manual as well as automated files and is in addition to the 21 million records in the files of the Federal Bureau of Investigation *See* Comptroller Gen. of the United States, *How Criminal Justice Agencies Use Criminal History Information,* August 1974. There are only 12 million records required nationally to account for first time and repeat offenders. Technical Rep. No. 14 *supra.* Therefore, the number of records actually stored indicates that records are being held in duplicate form in any number of files.

> by acquittal or complete exoneration of the charges involved. An arrest record may be used by the police in determining whether subsequently to arrest the individual concerned, or whether to exercise their discretion to bring formal charges against an individual already arrested. Arrest records have been used in deciding whether to allow a defendant to present his story without impeachment by prior convictions, and as a basis for denying release prior to trial or an appeal; or they may be considered by a judge in determining the sentence to be given a convicted offender.[4]

There have been attempts by some courts to minimize the adverse impact on the individual arising out of the dissemination of arrest records. In *Paul v. Davis*,[5] Justice William Brennan observed in a dissenting opinion that: "A host of state and federal courts, relying on both privacy notions and the presumption of innocence, have begun to develop a line of cases holding that there are substantive limits on the power of Government to disseminate unresolved arrest records outside the law enforcement system."[6]

The adverse impact of unlimited dissemination goes beyond arrest records to conviction records as well and some states have enacted laws limiting the dissemination of conviction information outside the criminal justice system.[7] A great deal has been written with regard to limiting dissemination of all forms of criminal history record information outside of the criminal justice community, and the potential harm to the individual from such dissemination has been well documented.[8] Criminal history record information includes information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, sentencing, correctional supervision, and release. The term does not include intelligence, investigative, or correctional information — probation reports, evaluative matters, etc.

Over the past number of years there has been much debate concerning the public's right to know the content of criminal history

---

4. Menard v. Mitchell, 430 F.2d 486, 490-91 (D.C. Cir. 1970) (footnotes omitted).
5. 424 U.S. 693 (1976).
6. *Id.* at 735 n.18 (Brennan, J., dissenting).
7. LAW ENFORCEMENT ASSISTANCE ADMIN., OFFICE OF GEN COUNSEL, U.S. DEP'T. OF JUSTICE, COMPENDIUM OF STATE LAWS GOVERNING THE PRIVACY AND SECURITY OF CRIMINAL JUSTICE INFORMATION (1975).
8. *Security and Privacy of Criminal Arrest Records, Hearings on H.R. 13315 Before Subcomm. No. 4 of the House Comm. on the Judiciary*, 92d Cong., 2d Sess. (1972) (Sup. Doc. No. Y4. J89/1: 92-27 P).

records and the privacy interests of the individual in limiting the dissemination of such records outside the criminal justice system. In the spring of 1975, the Law Enforcement Assistance Administration (LEAA) pursuant to a statutory amendment to its enabling legislation[9] issued regulations which had provisions setting limits on the dissemination of criminal history information. The dissemination provisions of the regulations[10] only permitted noncriminal justice agencies access to criminal history record information where a statute or executive order expressly referred to criminal conduct and contained requirements and/or exclusions based upon such conduct.

After these regulations were issued, strong protest against such stringent limitations began to surface and LEAA held public hearings in December of 1975[11] in which the press, private security personnel, and employers in varied areas, such as utilities, drug companies, etc., testified in opposition to the regulations. The major concerns expressed at the hearings on "dissemination" were on the need for conviction data for employment, licensing, and other related purposes, and the potential conflict of the regulations with state "public record" laws.

The private industry spokesmen who appeared at the hearings were primarily concerned with the need to know, before the fact, whether or not a present or prospective employee might constitute a threat to the lives or property of those with whom he works or to the public at large.

---

9. In 1973, the LEAA Act came before Congress for renewal. Senator Kennedy introduced an amendment to the Act calling for LEAA to assure the security and privacy of information contained in criminal justice information systems funded by LEAA. This amendment was enacted into law as section 524(b) of the Crime Control Act of 1973 and states as follows:

> 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 is adequately provided for and that 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.

Crime Control Act of 1973, Pub. L. No. 93-83, 87 Stat. 197 (amending 42 U.S.C. §§ 3701-3795 (1970)).

10. 28 C.F.R. § 20.21(b) (1975).

11. LEAA Dissemination Hearings, Federal Trade Building, December 11, 12, and 15, 1975.

Those companies whose employees regularly enter the homes of customers for the purpose of service calls or installations of equipments, gas, electric, telephone companies, were particularly concerned. One spokesman stated:

> In connection with its supply of gas and electricity to members of the general public, this company is vitally concerned in obtaining and retaining employees of high caliber who do not have criminal records so that we are in a position to assure ourselves and our customers that employees of this company who enter their homes on Company business, e.g., reading of meters, activating and terminating service, customer relations contacts, etc., are trustworthy and reliable. Hence, we are opposed to any limitations being imposed upon us . . . with respect to obtaining records relating to criminal conduct.[12]

Other private industry spokesmen were concerned over court decisions which appeared to put the burden of responsibility on private industry for acts committed by their employees under the doctrine of *respondeat superior*. A specific case mentioned at the hearings was the civil judgment awarded in mid-1974 by a U. S. District Court jury in the District of Columbia[13] to a rape victim who had sued an appliance firm and a trucking firm as a result of the attack. The assailant, an employee of the trucking company, was making deliveries for the appliance dealer. To the private firms that testified at the public hearings, it appeared paradoxical that employers were being held liable at law for the criminal acts of their employees, but were unable to review criminal record data in order to determine potential employees' character, reliability, and history.

Major drug companies, manufacturing and distributing drugs designated as "controlled substances" by the Controlled Substances Act[14] advised LEAA that they had serious legal responsibilities under that statute and under regulations and policies of the Drug Enforcement Administration (DEA) which were being undermined by their inability to obtain information as to the criminal convictions of applicants for employment who would have access to the controlled substances. They pointed out that in order to maintain

---

12. *Id.*

13. Lyon v. Carey, 385 F. Supp 272 (D.D.C. 1974). After the jury verdict, a motion to set aside notwithstanding the judgment was granted by the district court. The court held that the employee's action was not within the scope of employment. 385 F. Supp. at 274. On appeal the decision was modified as to defendant trucking company, the appellate court holding that the action was within the outer bounds of *respondeat superior*. 533 F.2d 649, 651 (D.C. Cir. 1976).

14. Pub. L. No. 91-513, 84 Stat. 1242 (1970) (codified in scattered sections of 21 U.S.C.).

effective controls against the diversion of controlled substances into other than legitimate channels, the DEA Manual for Drug Security contained the following section concerning employee screening: "Pre-employment screening for the purpose of identifying potential security problems is an important factor when choosing new employees for work in or around areas where controlled substances are handled. . . . Criminal background checks with local law enforcement authorities as well as with BNDD [Bureau of Narcotics and Dangerous Drugs] are equally important."

The drug manufacturers pointed out the obvious conflict between the DEA requirements and the limitations being imposed upon state and local law enforcement agencies by the LEAA regulations.

A representative of the Metropolitan Washington Board of Trade submitted for the record the results of its survey concerning the degree of internal employee thievery in the Metropolitan Washington area. Of the 106 firms surveyed, 9.4% responded to the questionnaire. Of those responding, 63.2% indicated known losses from confessed or apprehended employees in 1973, 1974, and 1975. The retail firms reported that they had apprehended 1,833 employees in 1973, 1,841 employees in 1974 and for the first nine months of 1975, 1,693 employees. The known losses attributable to these apprehended employees were $319,547 in 1973, $230,873 in 1974 and $377,536 for the first nine months of 1975. The firms reporting internal losses included those classified as associations, auto repair shops, communications firms, contracting firms, engineering firms, hospitals, real estate agencies, rental firms, restaurants, retail shops, savings and loan associations, schools and transportation firms.

In summary, the hearing record was replete with testimony regarding employers' need for access to criminal history record information in order to prevent: 1) Bodily injury caused by employees and; 2) Theft of money and merchandise.

Of the over 100 persons who either testified or submitted written comments on the dissemination provisions the record was clear that there was little, if any, support for the restrictive provisions of the regulations as they were originally promulgated on May 20, 1975. However, one of the more significant developments in the hearings was the fact that most of the representatives of private employers who appeared and presented statements did not ask for access to arrest records. These individuals asked only for access to conviction information. The representative of the American Telephone and Telegraph Company went even further and stated that AT&T wanted access to conviction records only for individuals being placed in a sensitive position.

Faced with a limited statutory mandate and lack of public support, LEAA revised the regulations. Under the revised regulations, there are no limits on the dissemination of conviction data. Nonconviction data[15] cannot be disseminated unless authorized by law, executive order, court rule, order or decision.[16] States are free to determine appropriate provisions for dissemination of criminal history record information.[17] Similar to the earlier regulations, the revised regulations contemplate that each state will examine its current practices for the dissemination of criminal history record information and will add provisions necessary for modifying those practices which are found to be in the best interests of that particular state.

While the focus in much public discussion has been that noncriminal justice access[18] to criminal justice information is the greatest hazard to the individual, the LEAA experience is just one of the many attempts to limit such access that has met with resistance. Numerous bills which would have limited dissemination of criminal history information have been introduced in Congress since 1971,[19] and while lengthy hearings have been held numerous times,[20] none of the bills has ever been voted out of the subcommittees. There have been similar experiences in many states. In Pennsylvania, the State's Security and Privacy Plan prepared by the Governor's Task Force on Criminal Justice Information Systems proposed strict limits on dissemination and the plan met with great resistance. The public debate in the summer of 1976 was sharp and divisive and hearings have since been held to consider legislation governing the dissemination of criminal history information.

---

15. 28 C.F.R. § 20.3(k) (1976) states as follows:
"Nonconviction data" means arrest information without disposition if an interval of one year has elapsed from the date of arrest and no active prosecution of the charge is pending; or information disclosing that the police have elected not to refer a matter to a prosecutor, or that a prosecutor has elected not to commence criminal proceedings, or that proceedings have been indefinitely postponed, as well as all acquittals and all dismissals.
Id.

16. 41 Fed. Reg. 11,714 (1976) (revising 28 C.F.R. § 20.21(b)).

17. 28 C.F.R. §20.21(c)(3) (1976).

18. Noncriminal justice access refers to any agency or individual not a part of the official public criminal justice system.

19. *See* 91st Cong., 1st Sess., H.R. 10789, H.R. 10892 and S. 2964 (1969); 93rd Cong., 2d Sess., H.R. 12574, H.R. 12575/ S. 2963 and S. 4252 (1974); 94th Cong., 1st Sess., H.R. 61/S. 1428 and H.R. 62/ S. 1427, S. 2008 (1975).

20. *See, e.g., Data Banks, Computers and the Bill of Rights, Hearings Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary,* 92d Cong., 1st Sess. (1971) (Sup. Doc. No. Y4.J89/2:B22/16); *Criminal Justice Data Banks — 1974, Hearings Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary,* 93d Cong., 2d Sess. (1974) (Sup. Doc. No. Y4.J89/2:C86/13/974 v.1).

The LEAA amendment,[21] the Privacy Act of 1974,[22] and an amendment to the law providing appropriations for the FBI,[23] contain the only specific federal statutory pronouncements in this area. These provisions do not at the present time provide the national framework necessary to limit dissemination of records.

It is clear that there is no overwhelming support for limiting dissemination of criminal history record information, and if an individual is not to be unnecessarily harmed by the dissemination of criminal history information, it is imperative that we look at what can be done to provide the degree of security and privacy necessary for criminal records and assure their integrity.

It must first be noted that by far the greatest use made of criminal history records is by criminal justice agencies. The Comptroller General of the United States conducted an investigation of the uses made of criminal history information.[24] A random sample of requests for criminal history information over a one-week period was obtained from data centers maintained by the FBI and the states of California, Florida and Massachusetts.[25] The study concluded that by far the greatest use made of this information was for post-arrest purposes. While some use was made by law enforcement agencies for records prior to arrest — suspicious circumstances arousing police interest, followup investigation before arrest — the uses made for specific post-arrest purposes were of greater significance. Such uses include: followup investigation after arrest, prosecution of suspect, plea bargaining, recommending or setting bail, sentencing, establishment of treatment programs while

---

21. *See* note 9 *supra*.

22. Privacy Act of 1974, 5 U.S.C. § 552a (Supp. V 1975). Criminal justice information is addressed by the Act insofar as federal records are concerned, but does not cover state and local records, nor does it cover federal court records. There is an exemption which may be utilized by a federal agency to limit the applicability of the Act's provisions. 5 U.S.C. § 552a(j), (k) (Supp. V 1975).

23. Pub. L. No. 92-544, 86 Stat. 1115 (1972) prohibits the exchange of identification records by the FBI except with "officials or federally chartered or insured banking institutions . . . and, if authorized by State statute and approved by the Attorney General, to officials of State and local governments for purposes of employment and licensing, any such exchange to be made only for the official use of . . . such official." *Id.*

24. Comptroller General of the United States, *How Criminal Justice Agencies Use Criminal History Information,* August 1974. In March 1974 the Senate Subcommittee on Constitutional Rights held hearings on proposed legislation to guarantee the security and privacy of criminal history record information. The subcommittee requested that Government Accounting Office determine the extent of the use of criminal history record information by criminal justice agencies. *Hearings on S.2963 & 2964 Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary,* 93d Cong., 2d Sess (1974) (Sup. Doc. No. Y4.J89/2:C86/13/974 v.1).

25. This did not include files maintained locally by the criminal justice agencies of these states but only the state data centers.

in a correctional institution, parole decisions, and supervision requirements after release of defendant on parole or probation. The decisions made by the criminal justice community based upon criminal history records in each of these areas can be critical. In 1975 approximately sixty-eight million requests were made for criminal histories by state and local level criminal justice agencies. Of the criminal histories received 31% had missing data and 10%, it was estimated, had erroneous information.[26]

It is obvious that reliance on incomplete or inaccurate data can cause great harm to the individual. Privacy has been defined in various ways. One of the best definitions, for our purposes, is found in the National Advisory Commission on Criminal Justice Standards and Goals Report on Criminal Justice System. The Commission defines privacy as "protection of the interests of the people whose names appear for whatever reason in the contents of a criminal justice information system."[27] Protection of such interests will be enhanced when methods are in place to insure completeness and accuracy of data. The Commission recommended that the following methods be established:

1. Every item of information should be checked for accuracy and completeness before entry into the system. In no event should inaccurate, incomplete, unclear, or ambiguous data be entered into a criminal justice information system. Data is incomplete, unclear, or ambiguous when it might mislead a reasonable person about the true nature of the information

2. A system of verification and audit should be instituted. Files must be designated to exclude ambiguous or incomplete data elements. Steps must be taken during the data acquisition process to verify all entries. Systematic audits must be conducted to insure that files have been regularly and accurately updated. Where files are found to be incomplete, all persons who have received misleading information should be immediately notified.

Senator Kennedy, the sponsor of the amendment to the Omnibus Crime Control and Safe Streets Act — section 524(b),[28] — was most concerned with the inaccuracy and incompleteness of criminal history record information. One of the most important areas dealt with by the LEAA regulations implementing section 524(b) involves insuring completeness and accuracy of criminal history record

26. *See* Technical Rep. No. 14, *supra* note 3.

27. U.S. NATIONAL ADVISORY COMM'N. ON CRIMINAL JUSTICE STANDARDS AND GOALS, REPORT ON THE CRIMINAL JUSTICE SYSTEM, 114 (1973) (Sup. Doc. No. Y3.C86:2C86/2).

28. Crime Control Act of 1973, Pub. L. No. 93-83, 87 Stat. 197, (amending 42 U.S.C. § 3701 (1970)).

information. The regulations define completeness as requiring dispositions made within the state to be posted to the record held by state repositories within ninety days of their occurrence.[29] A disposition is defined as information disclosing that

> criminal proceedings have been concluded, including information disclosing that the police have elected not to refer a matter to a prosecutor or that a prosecutor has elected not to commence criminal proceedings and also disclosing the nature of the termination in the proceedings; or information disclosing that proceedings have been indefinitely postponed and also disclosing the reason for such postponement. Dispositions shall include, but not be limited to, acquittal, . . . acquittal by reason of mental incompetence, case continued without finding, charge dismissed, charge dismissed due to insanity, charge dismissed due to mental incompetency, charge still pending due to insanity, charge still pending due to mental incompetence, guilty plea, nolle prosequi, no paper, nolo contendere plea, convicted, youthful offender determination, deceased, deferred disposition, dismissed — civil action, found insane, found mentally incompetent, pardoned, probation before conviction, sentence commuted, adjudication withheld, mistrial — defendant discharged, executive clemency, placed on probation, paroled, or released from correctional supervision.[30]

An ideal method to provide for complete records would be to enact mandatory requirements for reporting dispositions to a central repository of criminal history information and for assuring that arrest information is not disseminated without available information on the disposition of the arrest. The National Advisory Commission on Criminal Justice Standards and Goals recommended that such repositories be located at the state level because of considerable intrastate mobility of offenders.

The regulations encourage the establishment of central state repositories and provide that in those states which have central state repositories "procedures shall be established for criminal justice agencies to query the central repository prior to dissemination of any criminal history record information to assure that the most up-to-date disposition data is being used."[31] Although exceptions are permitted where manual systems cannot respond quickly enough, such exceptions apply only until the central state repository can be upgraded to a level of technical capability that will enable them to respond in a reasonable time for every inquiry.

29. 28 C.F.R. § 20.21(a)(1) (1976).
30. *Id.* § 20.3(e).
31. *Id.* § 20.21(a)(1).

The minimum requirements, concerning disposition reporting and predissemination inquiries to insure the most current records, are based upon the premise that every state will eventually have a central repository and that complete records will be stored there and not in local files. In the event that criminal history records are maintained in local criminal justice agency files, they are subject to the requirement that records available for dissemination must include dispositions to the maximum extent feasible.

The regulations define "accuracy" to mean that no record containing criminal history record information shall contain erroneous information.[32] A systematic audit is required by a repository as a means of insuring the completeness and accuracy of records. Accuracy checks require controls and inspections on the input to the system. Audits require entry verification and properly interpreted source documents. Audit trails[33] are to be established to guarantee that a maximum level of system accuracy is maintained.[34]

The traditional view of computer communications is that this technological advance will cause a loss of personal liberty because of the apparently limitless amount of information that can be collected and disseminated about an individual. Yet this very sophisticated information technology can lead to improved operations; the ease with which computers allow access to records has greatly increased the capability to correct records and will lead to more accurate recordkeeping. The standards which have been discussed can more easily be established because of the technological advances. The ability to maintain up-to-date records, to track dissemination flow so that any inaccuracies and challenged records can be immediately corrected, is made more feasible by computerization rather than manual recordkeeping. Instead of increasing file size and permitting redundant and obsolete records to exist in many different files throughout the state, computerization can be used to reduce data storage.

By 1985, a study has shown, a computerized criminal history system utilizing central state repositories if established by all fifty states could reduce the more than 195 million records distributed in varied criminal justice agencies to about twenty-five million records in state data centers.[35] A smaller system would permit greater control over the processing of data. The right of access to these data

---

32. *Id.* § 20.21(a)(2).

33. Audit trails are documentation sufficient to enable an auditor to trace the usages made of the data.

34. 28 C.F.R. § 20.21(a)(2) (1976).

35. *See* Technical Rep. No. 14, *supra* note 3, at 35.

banks by the individual whose records are maintained therein, so that he or she may challenge and correct the information being collected, would establish the integrity of the information more easily.[36]

There has been some significant case law at the federal level dealing with accurate records. The United States Court of Appeals for the District of Columbia, in the last few years, has spoken decisively on the issue of accurate records. In *Tarlton v. Saxbe*,[37] the court held that the FBI had a duty to prevent the dissemination of inaccurate arrest and conviction records. Safeguarding the accuracy of these records was of paramount importance. The court stated:

> [D]issemination of inaccurate criminal information without the precaution of reasonable efforts to forestall inaccuracy restricts the subject's liberty without any procedural safeguards designed to prevent such inaccuracies. . . . [G]overnment collection and dissemination of inaccurate criminal information without reasonable precautions to ensure accuracy could induce a levelling conformity inconsistent with the diversity of ideas and manners which has traditionally characterized our national life and found legal protection in the First Amendment.[38]

The decision was not founded on constitutional grounds but by an interpretation of the FBI's statutory authority as requiring the collection and dissemination of accurate information. The case was remanded to the district court and after a hearing, the district court held[39] that 1) the FBI must forward any challenge concerning the accuracy of a record to the local agency that submitted the record; 2) nonserious offenses must be deleted from all FBI criminal records; and, 3) a feasibility study should be conducted of available systems and procedures to enable the FBI to keep disposition entries reasonably current.[40]

---

36. The Criminal Justice Information Systems Regulations require that procedures be established by the state to insure the individual's right to access and review his criminal history record information for purposes of accuracy and completeness. The state must provide administrative review and necessary correction of any claim by the individual to whom the record relates, that the record is inaccurate or incomplete. The correcting agency must notify all criminal justice recipients of the corrected information. 28 C.F.R. § 20.21(g) (1976).

37. 507 F.2d 1116 (D.C. Cir. 1974).

38. *Id.* at 1123, 1124 (footnotes omitted).

39. Tarlton v. Saxbe, 407 F. Supp. 1083 (D.D.C. 1976).

40. *Id* at 1089. As to the first two items, regulations governing the dissemination of criminal history records provide as follows:

> (a) Criminal history record information maintained in any Department of Justice criminal history record information system shall include serious and/or significant offenses.
>
> (b) Excluded from such a system are arrests and court actions limited only to nonserious charges, e.g., drunkenness, vagrancy, disturbing the peace, curfew

Other cases of significance dealing with inaccurate records are *Maney v. Ratcliff*,[41] *United States v. Mackey*,[42] and *Shadd v. United States*.[43] In *Shadd v. United States*,[44] summary judgment was entered for the petitioner with regard to certain of the allegations brought by the petitioner of improper entries and inaccuracies in files. The court held that duplicative listing of certain charges and the lack of a disposition entry for a charge which had been disposed of twenty-seven months earlier violated even a minimal definition of the responsibility to maintain accurate files.[45]

In *United States v. Mackey*,[46] the court held that an arrest based solely upon National Crime Information Center (NCIC) information which was inaccurate when relayed to state arresting officers[47] and which had been inaccurate for five months, constituted denial of due process of law. Evidence seized subsequent to such an arrest and the basis of a new indictment was therefore suppressed. The court determined that "a computer inaccuracy of this nature and duration, even if unintended, amounted to a capricious disregard for the rights of the defendant as a citizen of the United States."[48]

In *Maney v. Ratcliff*,[49] plaintiff was arrested on three different occasions based upon a stale "fugitive from justice" entry in the NCIC originating from Baton Rouge, Louisiana authorities. Although no extradition documents were ever forwarded, the entry was not removed from NCIC by the authorities. The court stated: "These facts demonstrate that the defendants have caused plaintiff to be arrested and jailed on three occasions and have not proceeded to

---

violation, loitering, false fire alarm, nonspecific charges of suspicion or investigation, traffic violations (except data will be included on arrests for manslaughter, driving under the influence of drugs or liquor, and hit and run). Offenses committed by juvenile offenders shall also be excluded unless a juvenile offender is tried in court as an adult

28 C.F.R. § 20.32 (1976). The exclusions, however, do not apply to the number of manual records compiled prior to June 1975. However, as the information is converted from manual to computer, only serious offenses will be maintained. Section 20.34 provides for the individual's right to access criminal history information about himself contained in the FBI files and provides a procedure for obtaining corrections of such records. *Id.* § 20.34.

41. 399 F. Supp. 760 (E.D. Wis. 1975).

42. 387 F. Supp. 1121 (D. Nev. 1975).

43. 389 F. Supp. 721 (W.D. Pa. 1975).

44. *Id.*

45. *Id.* at 724.

46. 387 F. Supp. 1121 (D. Nev. 1975).

47. *Id.* at 1122. Defendant was hitchhiking when he was stopped by the police. His name and description was put on the NCIC computer and the return answer showed an outstanding fugitive warrant for violation of probation. This was the sole cause of his arrest. During the booking, an illegal firearm was found in the defendant's duffle bag. Possession of the weapon was the basis of the subsequent charges. *Id.*

48. *Id.* at 1125.

49. 399 F. Supp. 760 (E.D. Wis. 1975).

extradite him by the proper lawful procedures. The violation of plaintiff's rights by the capricious actions of the defendants [Louisiana officials] is unquestionable."[50]

The courts seem clear in their emphasis that due process requires reliance on accurate records and that where such records are not accurate, subsequent decisions based upon such records may be considered defective. With regard to the question of limiting dissemination of records where the question of accuracy or completeness has not been an issue, the courts have wrestled with the problems of prior restraint and the "public's right to know" and have denied the claims of privacy. In *Paul v. Davis*,[51] the Supreme Court held that distribution of a flyer captioned "Active Shoplifters" with names and photographs of an individual arrested but not convicted for shoplifting could be circulated without violating any provision of the Constitution. In *Tennessean Newspaper, Inc. v. Levi*,[52] a case arising under the Privacy Act of 1974,[53] the court characterized the privacy concerns of indicted or arrested persons to be minimal and denied the government's contention that the Privacy Act prohibited disclosure of background information being requested by Tennessean Newspaper on individuals indicted and arrested for federal offenses. The court set out a test for determining the validity of a Privacy Act claim; the threshold question is whether the potential invasion of privacy involves minimal or substantial privacy concerns.[54] If the concerns are minimal, disclosure is mandated. If the concerns are substantial, then the court will employ a balancing test, weighing the public interest purposes served by disclosure versus the extent of individual privacy loss.

In the instant case, plaintiff prevailed when the court characterized the privacy concerns of indicted or arrested persons to be minimal. The court flatly stated that such individuals' lives are "no longer truly private."[55] Thus, the court did not need to balance competing considerations. The court stated in particular:

> Disclosing the requested information about persons arrested or indicted for federal criminal offenses does not involve substantial privacy concerns. Several factors support this conclusion. . . . [I]ndividuals who are arrested or indicted become persons in whom the public has a legitimate interest, and the basic facts which identify them and describe generally the investigations

50. *Id.* at 773.
51. 424 U.S. 693 (1976). *See* note 5 and accompanying text *supra*.
52. 403 F. Supp. 1318 (M.D. Tenn. 1975).
53. 5 U.S.C. §552a (Supp. V 1975).
54. 403 F. Supp. at 1320-21.
55. *Id.* at 1321.

> and their arrests become matters of legitimate public interest. The lives of these individuals are no longer truly private. Since an individual's right of privacy is essentially a protection relating to his or her private life, this right becomes limited and qualified for arrested or indicted individuals, who are essentially public personages.[56]

Another element necessary to safeguard the system is securing the data centers from unauthorized access. Even if dissemination were allowed without limit, it would still be necessary to insure that only authorized personnel could input into the system and retrieve information from it. Information must be properly processed and stored in the system. Assuring integrity of the data requires that the system site, whether manual or computer, have adequate physical security to protect against any unauthorized personnel gaining access to the stored data to modify, change, update, or destroy such information.[57] Physical security also includes developing procedures to protect the information from natural or man-made hazards or disasters. These procedures include screening of personnel, use of guards, badges, passwords, sign-in logs, as well as designing facilities to reduce the possibility of physical damage to the information.

In summary, efficient recordkeeping procedures and management which focus upon completeness and accuracy of the records maintained by criminal justice agencies will provide certain minimum safeguards necessary to protect the interests of the people whose records are maintained in a criminal justice information system and provide that the decisions made, whether by law enforcement agencies or by nonlaw enforcement agencies, are based upon accurate and complete records. Comprehensive legislation is needed to settle the sensitive issues raised by limiting dissemination. Until Congress deals dispositively with those issues, the main protection available to an individual is assuring accurate and up-to-date criminal history record information.

---

56. *Id.* (footnote omitted).

57. For further information regarding procedures, *see Criminal Justice Computer Hardware and Software Considerations,* Technical Memorandum No. 6, SEARCH Group, Inc., Sacramento, Cal. (1974).