UIC John Marshall Journal of Information Technology & Privacy Law

Volume 6
Issue 4 *Computer/Law Journal - Spring 1986*

Article 3

Spring 1986

Data Accuracy in Criminal Justice Information Systems: The Need for Legislation to Minimize Constitutional Harm, 6 Computer L.J. 677 (1985)

Mark A. Beskind

NOTES

DATA ACCURACY IN CRIMINAL JUSTICE INFORMATION SYSTEMS: THE NEED FOR LEGISLATION TO MINIMIZE CONSTITUTIONAL HARM

The computer and information revolution began affecting the criminal justice process twenty years ago. Today, government agencies collect, store, collate, and use vast amounts of information about citizens. At all levels of government, law enforcement agencies and an increasing number of non-criminal justice agencies are making use of data in computer systems such as the National Crime Information Center ("NCIC").

Since its inception in 1967, NCIC has improved its operations significantly. New policies, procedures, and applications for the system are constantly studied. NCIC has proved to be a highly useful tool for distributing information about wanted or missing people and stolen property. In general, however, the system's authority and guidelines for use are broad and vague. Compliance with procedures is low, and there are inadequate enforcement mechanisms.

These problems have caused data accuracy in NCIC to suffer. Accuracy is improving, but only slowly. Poor criminal justice data quality leads to two problems: first, individual constitutional rights may be violated by the use and dissemination of inaccurate data; second, the effectiveness of a valuable criminal justice tool is diminished. These problems are even more pressing given the potential for surveillance applications of this technology.

This Note examines the NCIC system and the quality of its data. The author argues that the use and dissemination of inaccurate data violates the constitutional rights of due process, privacy, the presumption of innocence, and equal protection of the laws. The Note illustrates how system effectiveness is reduced in the process of violating these rights. Current policies and procedures are reviewed. Finally, the author concludes that comprehensive national legislation should be

passed, including provisions to insure higher data quality, to minimize violations of constitutional rights, and to improve the system.

I. THE NCIC SYSTEM

NCIC is a computer system under the control of the Federal Bureau of Investigation ("FBI"). The system electronically links approximately 64,000 criminal justice agencies at all levels of government throughout the United States, Puerto Rico, the United States Virgin Islands, and Canada, providing a very useful tool for law enforcement agencies.[1] This network not only makes data from one jurisdiction available to another, but also makes it more difficult for criminals to escape the law.[2] NCIC permits law enforcement officers in the field to determine if individuals in their presence are wanted anywhere in the country, or if property has been reported stolen.

NCIC data are available to local law enforcement officers in a matter of seconds.[3] This speed, when coupled with the increased ability to locate criminals, permits "the administration of criminal justice [to] operate more rapidly and effectively than ever before."[4] NCIC provides "the criminal justice community [at all levels of government with] a central file [of] documented information on wanted persons, criminal histories, missing persons, and stolen property."[5]

NCIC contains twelve categories or files of data. Eleven of the files are known as "hot files." They provide a "bulletin board" capability to law enforcement agencies. Six of the "hot files" list stolen property of various types. Two other "hot files" contain data on missing and unidentified persons.[6] The most recently added and most controversial

---

1. *See* Burnham, *F.B.I. May Test Computer Index for White-Collar Crime Inquiries*, N.Y. Times, Oct. 25, 1984, at A1, col. 4; FBI, U.S. Dep't of Justice, NCIC Operating Manual, at Intro-1 (rev. 51 June 25, 1984) [hereinafter cited as Manual].

2. Note, *Gargage In, Gospel Out: Establishing Probable Cause Through Computerized Criminal Information Transmittals*, 28 HASTINGS L.J. 509, 510-11 (1976) [hereinafter cited as *Garbage In, Gospel Out*].

3. National Crime Information Center, FBI, U.S. Dep't of Justice, User Agreement pt. 2, at 3 (NCIC Standards, Apr. 1, 1984) [hereinafter cited as User Agreement].

4. FBI, U.S. Dep't of Justice, Make NCIC Work for You, at introduction inside front cover (rev. Feb. 1983).

5. FBI, U.S. Dep't of Justice, National Crime Information Center: The Investigative Tool, at I (June 1984) [hereinafter cited as Investigative Tool].

6. The stolen property files include information about vehicles, license plates, boats, and guns; articles such as televisions, radios, and office equipment; and securities. FBI, U.S. Dep't of Justice, NCIC Newsletter 3 (Winter 1984) (Chart of NCIC File Size) [hereinafter cited as File Size Chart]. *See also* Investigative Tool, *supra* note 5, at 3; FBI, U.S. Dep't of Justice, Extradition of Wanted Persons and the National Crime Information Center 1 (June 1, 1983) [hereinafter cited as Extradition of Wanted Persons]; OFFICE OF TECHNOLOGY ASSESSMENT, U.S. CONGRESS, AN ASSESSMENT OF ALTERNATIVES FOR A NA-

file concerns people who are deemed a threat to Secret Service protectees.[7] Another "hot file" lists people wanted pursuant to Canadian warrants. The eleventh "hot file," which is a subject of this Note, is the Wanted Persons File ("WPF"). This file lists information on wanted persons throughout the United States.[8]

NCIC contains another file which is a subject of this Note: the Computerized Criminal Histories file ("CCH").[9] In contrast to the "hot files," CCH is archival in nature. It is one example of a national computerized criminal history system. The CCH design creates a central repository of criminal history information on individuals, which is available to authorized recipients. These records are analogous to "rap sheets."

This Note also discusses the Interstate Identification Index ("III"), an alternative design to CCH for a national computerized criminal history system under the control of the FBI. NCIC is currently testing and implementing an III program. In contrast to CCH, which maintains all records in a central repository, III maintains criminal histories only for

---

TIONAL COMPUTERIZED CRIMINAL HISTORY SYSTEM 42 (1982) (Sudoc. No. Y3.T 22/2.2 C 86/2) [hereinafter cited as OTA REPORT].

7. The Secret Service file was approved by the Department of Justice and the FBI in September 1982. A file of this nature utilizes NCIC as a surveillance tool, to gather intelligence information on persons not formally charged with crimes. OTA REPORT, *supra* note 6, at 15 n.*. The Secret Service file became operational on April 27, 1983. The first "hit," or positive response, occurred two hours and seventeen minutes after the file was entered into the system. As of October 1983, there were records on 94 people, and 88 hits had occurred. Thirty-nine of those hits concerned people whose whereabouts at the time were unknown. FBI, U.S. Dep't of Justice, Minutes: National Crime Information Center Advisory Policy Board 2 (Oct. 5-6, 1983). *See also* FBI, U.S. Dep't of Justice, New File Promptly Proves Value, NCIC Newsletter 2 (Summer 1983). As of Februrary 29, 1984, the file contained 96 records. File Size Chart, *supra* note 6. Currently, the FBI is tracking approximately 125 people with the Secret Service file. The file continues to generate numerous hits, and has proved to be an effective surveillance tool. Telephone interview with Fred B. Wood, Project Director, Office of Technology Assessment, U.S. Congress, (Mar. 26, 1985) (based on information provided to him by the FBI).

Other recent FBI proposals suggest that the agency is interested in using the intelligence capabilities of the system. For example, the FBI wants to add a file of white-collar crime suspects. Burnham, *supra* note 1. The FBI also sought to add information on people not wanted for specific crimes, but suspected as drug traffickers, terrorists, or associates of wanted persons. FBI Director William H. Webster rejected this proposal in 1984. Burnham, *supra* note 1, at B17, col. 2.

8. *See* Investigative Tool, *supra* note 5, at 3, 31-32.

9. *See generally* OTA REPORT, *supra* note 6 (discussing and analyzing CCH and alternative computerized criminal history systems). Until February 1984, NCIC maintained a "Criminalistics Laboratory Information System/General Rifling Characteristics" file. This file was a data base of scientific reference information, containing no information on individuals. As of February 1984, the data are no longer on-line; data are available, however, in hard-copy printouts. FBI, U.S. Dep't of Justice, CLIS Going Off Line, NCIC Newsletter 3 (Fall 1983).

federal offenders in the NCIC system, coupled with a list or index of state offenders by name. Under this approach, records of state offenders are maintained in state computer systems.[10] The index of state offenders also includes descriptive information, such as height and weight, and identification numbers, such as social security and criminal identification numbers.[11]

III was developed in response to concerns over control of CCH data, and has been endorsed by the NCIC Advisory Policy Board. State and local law enforcement officials and others prefer the decentralized design of III to CCH.[12] "Because about 95 percent of records exchanged by the III are likely to be State records, the States have generally sought a major role in policy control."[13] As a result of the success of the III test program, NCIC no longer refers to the CCH file, and the FBI plans to replace the CCH design with the III file. To avoid confusion, however, this Note refers to these files separately.

The current statutory authority for NCIC is very broad. In pertinent part, the statute provides:

> (a) The Attorney General shall—
>
> (1) acquire, collect, classify, and preserve identification, criminal identification, crime, and other records; [and]
>
> . . . .
>
> (4) exchange such records and information with, and for the official use of, authorized officials of the Federal Government, the States, cities, and penal and other institutions.[14]

On its face, the statute offers no guidance for the use or control of the system. In fact, the statute does not specifically authorize the NCIC system. It makes reference to neither NCIC nor the FBI, the federal agency which oversees the system.[15] The statute does not outline the

---

10. OTA REPORT, *supra* note 6, at 4. As of May 1983, 15 states and the federal government participated in the III program. *The National System for Interstate Exchange of Criminal History Records: Hearing Before the Subcomm. on Patents, Copyrights and Trademarks of the Senate Comm. on the Judiciary*, 98th Cong., 1st Sess. 64 (1983) (statement of Kier T. Boyd, Deputy Assistant Director, Technical Services Division, Federal Bureau of Investigation, Department of Justice) [hereinafter cited as *Hearings*].

11. *See* OTA REPORT, *supra* note 6, at 17.

12. OTA REPORT, *supra* note 6, at 10, 16, 118. Search Group, Inc., an organization that has studied criminal justice computer systems for years, has also endorsed the III design. *See Hearings*, *supra* note 10, at 149 (statement of William C. Corley, member, Board of Directors of Search Group, Inc., and director, police information network of North Carolina).

13. *Hearings*, *supra* note 10, at 17 (statement of Fred B. Wood, Project Director, Office of Technology Assessment, United States Congress).

14. 28 U.S.C. § 534(a) (1982).

15. On January 20, 1966, the Attorney General approved development of NCIC under the control of the FBI. Initially, only wanted person and stolen property data were included. "[T]he Attorney General cited the FBI's collection and exchange of criminal

types of identifying characteristics that the records may contain. It indicates neither the purpose for collecting the information nor the uses for the records. There is no assignment of responsibility for the accuracy or update of the records.

The statute does state that records will be disseminated, but only broad categories of recipients are listed. The statute also fails to describe how the records should be used. In fact, the only limitation on data use is that "[t]he exchange of records and information . . . is subject to cancellation if dissemination is made outside the receiving departments or related agencies."[16]

This sanction is not very effective. First, improper dissemination does not automatically impose the sanction. Second, the provision is silent as to which agencies or officials should police dissemination. There is no indication of who will decide to cancel system access. Finally, there is no provision to recover records from an unauthorized recipient. Indeed, one court noted that, in connection with the FBI's Identification Division (depository for the manual fingerprint and criminal record files maintained pursuant to the same statute), the FBI "has not aggressively policed use of its records . . . and has in fact, since 1924, suspended the privileges only of six local law enforcement agencies, none of them major departments."[17]

Fortunately, there are additional provisions which control NCIC. Federal regulations have been promulgated regarding the operation of the CCH file.[18] In addition, the FBI has formulated policies and procedures for use of the NCIC system. These requirements are found in the NCIC User Agreement and the NCIC Operating Manual.[19] These FBI policies place a great deal of importance on the accuracy, completeness, timeliness, and currentness of data. The FBI denies ultimate responsibility for data quality, however, although it manages and oversees the system, and despite the fact that the courts have placed some duty on

---

records with local police organizations as sufficient authority" for FBI development of NCIC. OTA REPORT, *supra* note 6, at 34. Approval for the development of CCH under the FBI came later. On December 10, 1970, the Attorney General decided that the FBI would be responsible for CCH, even though other agencies and organizations had been considered. *Id.* at 36. The Attorney General also delegated authority to the FBI in 28 C.F.R. § 0.85. OTA REPORT, *supra* note 6, at 62.

16. 28 U.S.C. § 534(b) (1982).

17. Menard v. Saxbe, 498 F.2d 1017, 1028 n.41 (D.C. Cir. 1974). As of May 1983, the absence of proper management and security control had led to denial of access to III records by users in two states. *Hearings*, *supra* note 10, at 74 (statement of Kier T. Boyd).

18. 28 C.F.R. §§ 20.30-.38 (1985).

19. User Agreement, *supra* note 3; Manual, *supra* note 1. The NCIC Advisory Policy Board develops and studies proposals to improve the system. NCIC procedures are based partially on the Board's recommendations. *See* OTA REPORT, *supra* note 6, at 66.

the FBI to maintain accuracy.[20] Furthermore, recent studies show that data stored in the WPF and CCH files is far from 100% accurate.[21] The FBI policies governing the use of the NCIC system will be discussed in detail after data quality problems and the potential for constitutional harms are explored.[22]

II. DATA INACCURACY IN THE NCIC SYSTEM

The concepts of accurate, complete, timely, and current data can include a variety of issues and problems which are interconnected. For example, assume an individual is arrested pursuant to a warrant, and the court takes some action. Further, assume the warrant is not removed from the WPF and a CCH record is created, but no one enters the court disposition. In this case, an invalid warrant remains in the system and an inaccurate, incomplete, and out-of-date CCH record exists. This example illustrates some of the types of "data inaccuracies" that impair the NCIC system.

A. WANTED PERSON FILE ("WPF")

Data inaccuracies are most easily discussed in the context of the WPF, CCH, and III files. As of October 1, 1981, the WPF contained 190,159 warrants—only 2.1% of all NCIC records.[23] However, WPF and three other "hot files" are used much more frequently than the other files; as of September 1981, these files together accounted for approximately 90% of all NCIC transactions.[24] Law enforcement officers believe that WPF is an invaluable tool.

The most serious data problem in the WPF file is the existence, use, and dissemination of information based on invalid warrants. An in-

---

20. *See* 28 C.F.R. § 20.37 (1985); OTA REPORT, *supra* note 6, at 66 n.3; Note, *Probable Cause Based on Inaccurate Computer Information: Taking Judicial Notice of NCIC Operating Policies and Procedures*, 10 FORDHAM URB. L.J. 497, 508 (1982) [hereinafter cited as *Probable Cause*]; *Garbage In Gospel Out*, *supra* note 2, at 529; Manual, *supra* note 1, at Intro-2, Intro-23; User Agreement, *supra* note 3, at 6-7; K. Laudon, Data Quality and Due Process in Large Inter-Organizational Record Systems 27-28 (rev. draft August 1984). *See also* cases cited *infra* note 170.

21. *See* OTA REPORT, *supra* note 6, at 87-96; K. Laudon, *supra* note 20.

22. *See infra* text accompanying notes 161-91.

23. OTA REPORT, *supra* note 6, at 42. As of February 29, 1984, WPF contained 210,899 records. File Size Chart, *supra* note 6.

24. The three other files contain data on stolen vehicles (12.5% of all records), stolen license plates (5.8% of all records), and missing persons (0.3% of all records). During September 1981, there were 10,270,500 NCIC transactions; the number of transactions in the WPF was not reported individually. OTA REPORT, *supra* note 6, at 42-43, 191. During February 1984, there were 12,392,454 transactions, or an average of 427,326 transactions per day. FBI, U.S. Dep't of Justice, NCIC Newsletter 2 (Winter 1984) (Chart of NCIC Transaction Volume).

valid warrant is one which appears to be outstanding but has actually been vacated or cleared. The existence of an invalid warrant makes an individual a "marked man" until the originating agency changes or deletes the record.[25] As a result, the individual is "subject to being deprived of his liberty at any time and without any legal basis."[26]

A recent study analyzed WPF record quality as of August 4, 1979. It found that 5.8% of the warrants sampled had been vacated prior to that date.[27] Another 5.1% of the warrants had been cleared or vacated, but the dates of clearance were unknown. For another 4.1% of the warrants, the originating agency had no record of issuing the warrant. Finally, no warrant could be located for wanted individuals in 0.8% of the records.[28] One of the contractors of this study, Professor Laudon, is in the process of further analyzing the results.[29] He estimates that the level of invalid warrants, when generalized to the WPF total population as of August 4, 1979, would amount to approximately 14,000 invalid warrants.[30]

Professor Laudon is also examining other aspects of data quality. His research indicates that the age of the warrant is another significant problem. He notes that 23.9% (approximately 30,000 warrants) are more than three years old, and 15.1% (approximately 19,000 warrants) are more than five years old. While the age of the warrant does not, in itself, prevent law enforcement officers from prosecuting the violations, prosecution becomes increasingly unlikely as time passes. District attorneys interviewed during the OTA study generally thought that five year old warrants could not be prosecuted, due largely to difficulty of proof, particularly locating witnesses.[31] Although prosecution may be unlikely, the chance of arrest or detention of the suspect is not dimin-

25. United States v. Mackey, 387 F. Supp. 1121, 1124 (D. Nev. 1975). Regarding the need for the originating agency to decide to alter a record, see Manual, *supra* note 1, at Intro-7, 7-14, 7-16, 7-24. WPF records may also be deleted when the wanted person is apprehended. *Id.* at Intro-10, 7-21 to 7-23. In addition, the FBI periodically purges the file. *Id.* at 7-3. Regarding the need for the originating agency to decide to alter or remove a CCH record, see 28 C.F.R. § 20.34 (1985); Manual, *supra* note 1, at Intro-7, 10-18 to 10-19; Tarlton v. Saxbe, 407 F. Supp. 1083 (D.D.C. 1976). *See also infra* text accompanying note 121.

26. *Mackey*, 387 F. Supp. at 1124.

27. OTA REPORT, *supra* note 6, at 192. The generalization of findings to the total number of warrants has a "95 percent confidence that the true parameters of record quality lie within plus or minus four percent of the estimates." *Id.* Of the warrants previously vacated, more than half had been vacated more than one month before the date of the study. Of those, more than half had been vacated at least six months earlier. *Id.*

28. OTA REPORT, *supra* note 6, at 192.

29. K. Laudon, *supra* note 20.

30. *Id.* at 19.

31. *Id.* at 19, 21, 28a. Another finding was that 6.6% (approximately 8,000 warrants) incorrectly classified the offense charged. Finally, the study concluded that 7% (approxi-

ished as long as the warrant remains in the system. If a decision not to prosecute is made because a warrant is too old, the originating agency should instruct the FBI to remove the warrant from the system. Removal of the warrant would insure that people are not detained or arrested for charges that will not be prosecuted.[32]

The studies of WPF record quality did not address other problems with WPF data, such as the lack of adequate identification information to describe the wanted person. Although this type of problem cannot properly be called an "inaccuracy," innocent individuals may be detained or arrested because they are mistaken for the wanted person. Perhaps the issue is better characterized as improper use of WPF data, or a failure by law enforcement officers to compare NCIC information with the originating agency's records. Illustrations will help to explain this problem, which this Note characterizes as "ambiguous" warrants.

Many warrants exist for individuals with common names. An innocent person with the same name may be stopped by the police, perhaps for a traffic violation. If the police query NCIC (or analogous state or local systems) and the response is a "hit" or positive response, the innocent individual will probably be detained and may be arrested. Other identifying characteristics, including the date of birth listed in the warrant, may be similar enough to those of the suspect to justify the detention or arrest. More importantly, however, the police may detain or arrest the innocent individual despite descriptive information in the warrant, such as an identifying scar, which shows that this person is not the wanted individual.

For example, B. William Jones was one of the named plaintiffs in a recently settled class action suit in Los Angeles.[33] Mr. Jones alleged that he was arrested or detained at least ten times within the three years preceding the filing of the case as a result of queries made by the police to the Automated Wants and Warrants System ("AWWS").[34] In

---

mately 8,000 warrants) contained such trivial charges that an apprehended suspect would not likely be prosecuted. *Id.* at 19, 21.

32. This procedure parallels the NCIC policy which requires a decision to extradite the wanted person before the warrant is entered into the system. If the jurisdiction of an originating agency does not want to extradite the wanted person, it makes no sense to have the warrant in a nationwide system. *See infra* text accompanying note 163. *See also* Manual, *supra* note 1, at 7-1; Maney v. Ratcliff, 399 F. Supp. 760 (E.D. Wis. 1975); Extradition of Wanted Persons, *supra* note 6.

33. Smith v. Gates, Civil No. CA000619 (Cal. Super. Ct. (Los Angeles County) Sept. 4, 1984) (stipulated judgment and order granting permanent injunction).

34. First Amended Complaint for Injunctive and Declaratory Relief and Damages para. 9, Smith v. Gates, Civil No. CA00619 (Cal. Super. Ct. (Los Angeles County) filed May 6, 1981) [hereinafter cited as Complaint]. AWWS is a computer system similar to NCIC. Although AWWS covers Los Angeles County, the system is linked to information available throughout California and the NCIC system.

one instance, Mr. Jones was incarcerated for twenty-six days until he was able to appear in each court that had issued a warrant. Each court determined, on the basis of simple handwriting comparisons or discrepancies in physical descriptions, that this Mr. Jones was not the wanted individual.[35] Furthermore, each time he was detained or arrested, Mr. Jones told the police that he was not the wanted person. Yet the officers "made no effort of any kind to determine whether or not J[ones] was in fact the person wanted, although information in the [police] files or otherwise readily accessible to them . . . would have demonstrated that J[ones] was not the wanted person."[36]

Another named plaintiff in the suit was subjected to malicious behavior and was subsequently arrested. An unknown person had told a bail bonding company that Martha Ramirez was the subject of a bench warrant for a "Bette Gonzales." Ms. Ramirez was turned over to the police and arrested, despite her repeated protests. Although she produced a valid Department of Motor Vehicles California Identification Card and another picture identification card, Ms. Ramirez was fingerprinted, photographed, booked, strip searched, and ordered to sign the name "Bette Gonzales" on her fingerprint card. The following day, the judge ordered the release of Ms. Ramirez, without even requiring fingerprint or handwriting comparisons, because she was obviously not the wanted person.[37] Apparently, the police made no effort to ascertain Ms. Ramirez' identity.[38]

Another type of "ambiguous" warrant may result if an individual's identification is lost or stolen. For example, in January 1981, Terry Rogan of Saginaw, Michigan lost his wallet in Detroit, Michigan. In a suit he has filed in federal district court, Mr. Rogan alleges that he was arrested five times (in Michigan and Texas) during the following two years because the Los Angeles police incorrectly entered a warrant for his arrest on murder and robbery charges, and subsequently failed to remove the warrant after they became aware of their error. Each time that he was arrested, calls to the Los Angeles police confirmed that Rogan was not the wanted person, but the warrant was not removed from

35. *Id.* para. 8.

36. *Id.* para. 11. Sheila Jackson, an Eastern Air Lines flight attendant, was similarly mistaken for a criminal who had violated parole in Texas. On October 28, 1983, Ms. Jackson returned to the United States on an Eastern flight from Mexico. Her passport was entered into NCIC by a customs official. Ms. Jackson was subsequently arrested on the basis of the NCIC hit and turned over to the Kenner, Louisiana police. Despite a five month discrepancy between Ms. Jackson's date of birth and that of the wanted criminal, the local police chief gave the benefit of the doubt to the computer information. Once Ms. Jackson was arrested, the police treated her like a criminal and refused to consider the possibility of an error. *See* ABC News, Transcript of 20/20 Broadcast 8-12 (Sept. 13, 1984).

37. Complaint, *supra* note 34, para. 16.

38. *Id.* para. 18.

NCIC until January 1984. At that time, police in Alabama arrested Bernard McKandis, the man who apparently had found Mr. Rogan's wallet and used Rogan's identification to create an alias.[39]

In addition to depriving innocent individuals of their liberty, dissemination of inaccurate WPF records also has negative effects on criminal justice efforts. First, inaccurate warrants waste law enforcement resources if the wrong individual is detained or arrested. Beyond the direct expenses of the unnecessary arrest and detention, the law enforcement agency may be liable for false arrest and the resulting damages. Furthermore, it can be argued that the administration of criminal justice may be frustrated by the dissemination of inaccurate warrants. For example, when an individual is arrested based on an inaccurate NCIC hit, other violations are sometimes discovered, such as possession of an illegal weapon or drugs. In some circumstances, the court may suppress the evidence of these other violations because they would not have been discovered absent the arrest based on the invalid warrant.[40] Thus, people who have actually committed crimes will not be punished. Of course absent the inaccurate hit, no arrest would have occured. Still, the fact remains that inaccurate hits do lead to arrests, which do waste law enforcement and criminal justice resources.

It would be difficult to determine how frequently these problems arise and how many innocent people are subject to wrongful arrests. This author knows of no studies that have been conducted on the subject. Nevertheless, there is no reason to assume that these are isolated incidents. At the very least, these cases demonstrate that police do not always follow NCIC procedures for the use of WPF data. Police sometimes do not believe people who claim they are not wanted, and do not check more reliable records that are easily available. Finally, it is clear that NCIC policies and procedures to insure data accuracy are inadequate and unenforced.

---

39. Ramos, *Couldn't Place Face, but Computer Never Forgot His Name*, L.A. Times, Feb. 13, 1985, pt. I, at 3, col. 1.

40. *See. e.g.*, United States v. Mackey, 387 F. Supp. 1121 (D. Nev. 1975); People v. Ramirez, 34 Cal. 3d 541, 668 P.2d 761, 194 Cal. Rptr. 454 (1983); Pesci v. State, 420 So. 2d 380 (Fla. Dist. Ct. App. 1982); People v. Lawson, 119 Ill. App. 3d 42, 456 N.E.2d 170 (Ct. App. 1983); Carter v. State, 18 Md. App. 150, 305 A.2d 856 (Ct. Spec. App. 1973); People v. Jennings, 54 N.Y.2d 518, 430 N.E.2d 1282, 446 N.Y.S.2d 229 (1981); People v. Lemmons, 49 A.D.2d 639, 370 N.Y.S.2d 243 (App. Div. 1975), *aff'd*, 40 N.Y.2d 505, 354 N.E.2d 836, 287 N.Y.S.2d 97 (1976); People v. Jones, 110 Misc. 2d 875, 443 N.Y.S.2d 298 (N.Y. City Crim. Ct. 1981). *But see* United States v. McDonald, 606 F.2d 552 (5th Cir. 1979); Childress v. United States, 381 A.2d 614 (D.C. 1977); Patterson v. United States, 301 A.2d 67 (D.C. 1973); Commonwealth v. Riley, 284 Pa. Super. 280, 425 A.2d 813 (Super. Ct. 1981).

B. COMPUTERIZED CRIMINAL HISTORY FILE ("CCH")

CCH accounts for a greater percentage of all NCIC records than does WPF; however, there are far fewer CCH transactions. As of October 1, 1981, CCH contained 1,885,457 records, 20.3% of all data.[41] In September 1981, however, CCH transactions were only 3.5% of the monthly total.[42]

The OTA Report analyzed a random sample of CCH record disseminations as of August 12, 1979, to verify a recent arrest in each record.[43] The most significant problem with CCH data is the lack of disposition information: cases in which the local record reflected a court disposition for the arrest, but the CCH record did not. The study found that 27.2% of the records showing verifiable arrests contained no disposition, even though disposition had occurred at least 120 days earlier.[44] The failure to report dispositions within 120 days is a direct violation of federal regulations.[45]

Another significant problem was inaccurate disposition, charging, or sentencing infomation; that is, the CCH information concerning these events did not agree with the local records. Disposition, charging, or sentence information was inaccurate in 19.4% of the records.[46]

The OTA Report may underestimate the extent of these problems. For example, the study excluded records from analysis if the arrest was

---

41. OTA REPORT, *supra* note 6, at 42. As of February 29, 1984, the file the FBI now calls the Interstate Identification Index contained 8,335,711 records. File Size Chart, *supra* note 6.

42. OTA REPORT, *supra* note 6, at 43.

43. The OTA Report results can be generalized to all 1979 CCH disseminations, but not to the entire CCH file. There is a 95% confidence that the record quality estimates are accurate within plus or minus 6%. OTA REPORT, *supra* note 6, at 90.

44. OTA REPORT, *supra* note 6, at 91. The verifiable records in the sample also included one arrest for which disposition had occurred within 120 days, and two arrests for which the date of disposition was unknown. *Id.* at 93. The FBI's own study found that as of August 13, 1979, 39.4% of arrests in the CCH had no dispositions. *Id.* at 91. In 1982, only 22 states had disposition reporting rates of 76 to 100%; in 12 states the rate was 51 to 75%; the rate in five states was 26 to 50%; and in eight states the rate was 0 to 25%. *Hearings*, *supra* note 10, at 55 (statement of Fred B. Wood). Of course, these statistics include data from manual state systems, which generally have lower disposition reporting rates than states with computerized systems. *Id.* at 56.

45. Criminal history records maintained in state repositories must reflect court disposition within 90 days after the disposition occurred. 28 C.F.R. § 20.21(a)(1) (1985). Responsibility for completeness, accuracy, and timeliness of CCH data in the NCIC system rests with the agency that submits the data. *Id.* § 20.37. "Dispositions should be submitted by criminal justice agencies within 120 days after the disposition has occurred." *Id.* "OTA found that, as of 1982, only 13 of 47 States are in substantial compliance with the Title 28 requirements for 90-day disposition reporting." *Hearings*, *supra* note 10, at 15 (statement of Fred B. Wood).

46. OTA REPORT, *supra* note 6, at 91.

pending, the disposition had been legally sealed, the arrest was not prosecuted, or no local record could be located. This last category of cases generally occurred when charges were dismissed after arrest, but before arraignment. Inability to locate a local record occurred in 16% of the records.[47] Thus, in 16% of the records, an individual had been arrested, released, and not charged, but a CCH record had been created.

Professor Laudon's further analysis of the OTA Report data found that approximately 54% of all CCH records contained some significant record quality problem. In 1978, there were approximately 360,000 CCH disseminations. Thus, Professor Laudon estimates that 194,760 disseminations (plus or minus 6%) were incomplete and/or inaccurate.[48]

The potential for CCH record quality problems becomes apparent when it is realized that only a handful of states are currently "full participants" in the CCH file. A state that is a full participant may not only receive CCH data, but also enter records into the file. No more than thirteen states have been full participants at any one time and, as of December 1981, only eight states were full participants.[49] As shown below, the level of record quality varies greatly among the states, and record quality in state systems is worse overall than in NCIC. It is reasonable to conclude that NCIC data quality would suffer if more states were full participants.[50]

Furthermore, the significance and effect of inaccurate CCH data depend on who is receiving the information and for what purpose. Recipients can be divided into two main categories: criminal justice agencies, and non-criminal justice agencies, including private organizations and individuals.[51]

---

47. OTA REPORT, *supra* note 6, at 91-92. In addition, the OTA Report results reflect only one quality problem per record, even though many records contained more than one problem. The study found that 6.7% of CCH records contained more dispositions than charges, or more charges than dispositions, compared to local records. *Id.* at 91.

48. Laudon, *supra* note 20, at 18 (table I), 19.

49. The eight states that were full participants in CCH as of December 1981, were Florida, Iowa, Michigan, Nebraska, North Carolina, South Carolina, Texas, and Virgina. The states that had been full participants are Arizona, California, Illinois, Minnesota, New York, Ohio, and Pennsylvania. OTA REPORT, *supra* note 6, at 43. As of December 1981, all states except Kansas participated in CCH to the extent of receiving data, but not contributing to the file. *Id.* at 43-44. As of June 25, 1984, 16 states were participants in the III program: California, Colorado, Florida, Georgia, Michigan, Minnesota, New Jersey, New York, North Carolina, Ohio, Oregon, Pennsylvania, South Carolina, Texas, Virginia, and Wyoming. An III participant is a state which the FBI permits to provide "records from its file [to inquiring agencies] upon receipt of notification from the NCIC III." Manual, *supra* note 1, at 10-23.

50. *See infra* text accompanying notes 58-66.

51. FBI statistics for 1981 on use of the manual Ident records break down as follows: federal criminal justice use, 3%; state and local criminal justice use, 44%; federal non-criminal justice use, 30%; and state and local non-criminal justice use, 23%. *See Hearings,*

Federal and state laws almost always permit dissemination of CCH data to criminal justice agencies regardless of its completeness or accuracy. Even if CCH information is incomplete or inaccurate, prosecutors believe that it is a useful "pointer" to more accurate data.[52] Records are used in charging, setting bail, sentencing, establishing parole, and in other facets of the process. While many judges will not consider violations committed in other jurisdictions without disposition information, if data are complete but inaccurate, an arrestee may be improperly charged with a more serious offense, or denied bail.[53]

Outside the criminal justice system, dissemination to federal, state, and local non-criminal justice agencies is allowed.[54] CCH data may be used in licensing and employment decisions.[55] The data may be disseminated without disposition information as long as the arrest charge is less than one year old. As of mid 1981, twenty-seven states permitted dissemination of CCH data to private organizations and individuals.[56]

In this context, the effect of inaccurate data may be even more serious than in the criminal justice context. Certainly, states and public employers have good reason for checking the criminal histories of potential employees: protection of the public. Private employers may be similarly justified, particularly if an individual is applying for a position of responsibility. If data are inaccurate, however, an individual could be

---

supra note 10, at 57 (statement of Fred B. Wood). The OTA REPORT found that the total use of CCH records by the 27 computerized states was as follows: law enforcement use, 56%; other criminal justice use, 29%; non-criminal justice use, 15%. *Id.*

52. OTA REPORT, *supra* note 6, at 95.

53. *Id.* at 128-34.

54. *Id.* at 95. State and local agencies may receive records without dispositions if authorized by state or federal statutes and approved by the U.S. Attorney General. Federal agencies may receive such records if authorized by federal statute or executive order. *Id.* The OTA study found that non-criminal justice use was as follows: state and local license applications accounted for 49% of non-criminal justice use; state and local employment checks, 24%; state and local security checks, 4%; and federal employment and security checks, 23%. *See Hearings*, *supra* note 10, at 57 (chart presented by Fred B. Wood). "[I]t is estimated that about 30 percent of the total work force, some 36 million Americans, have had some acquaintance with the criminal justice system, [and have] some kind of a record . . . ." *Id.* at 3 (opening statement of Senator Charles McC. Mathias, Jr., Chairman, Subcomm. on Patents, Copyrights and Trademarks of the Senate Comm. on the Judiciary).

55. 28 C.F.R. § 20.33 (1985). *See also infra* text accompanying notes 182-87. As of May 1983, non-criminal justice agencies did not have access to III data. It is likely, however, that III data will be available for non-criminal justice use in the future. To deny such access permanently would require that the FBI (or another agency) maintain a separate, duplicate file of state criminal history records for non-criminal justice purposes. "This would defeat one of the major objectives of the III in the first place, which is to get away from a national full record repository." *Hearings*, *supra* note 10, at 59 (statement of Fred B. Wood).

56. OTA REPORT, *supra* note 6, at 95.

unfairly denied employment. The situation could be particularly tragic if the individual had been mistakenly arrested on an inaccurate warrant, cleared of the charges, but a CCH file was created which lists the improper arrest or detention.[57]

C. INTERSTATE IDENTIFICATION INDEX ("III")

As described above, III is an alternative design to CCH to maintain computerized criminal history records.[58] Because III depends on state repositories to maintain records on non-federal offenders, the completeness and quality of data in state systems must be examined. Such an evaluation is difficult to accomplish because some states do not maintain computerized systems, and disposition reporting procedures vary. The OTA Report, however, did obtain some information and make some findings which give an indication of state criminal history record quality.[59]

The OTA Report focused only on disposition reporting and, based on the forty-one states that responded to the survey, found the average reporting level to be approximately 65%.[60] The study also found that an average of only 78% of arrests were reported. By 1982, when the follow-up survey was conducted, arrest reporting had increased to 82% and disposition reporting to 66%.[61]

In 1979, the average disposition reporting rate was higher for states with a CCH system or an automated name index — 71% compared to 50% for states with manual systems. At that time, twenty-nine states maintained computerized systems. The disposition reporting levels in

---

57. *See infra* text accompanying notes 143-46. Of course, technological advances could serve to limit or control dissemination of criminal history data for non-criminal justice purposes. It might be difficult, however, for the states and the federal government to agree on policy matters and access rules. It could be costly to reprogram the computer systems. In addition, these programming controls would be harder to implement in a decentralized III design, because NCIC would maintain only a name index of state offenders. The index would not list the types of offenses in a given record, nor would it indicate whether disposition information had been reported. Therefore, any search that resulted in a hit would require programming to route the request to the state repository which maintains the record, to determine if the record could be disseminated. This step would be necessary to prevent the requester from receiving a hit where no record could be disseminated. *See Hearings*, *supra* note 10, at 62 (statement of Fred B. Wood).

58. *See supra* text accompanying notes 10-13.

59. OTA REPORT, *supra* note 6, at 90-91. OTA sent a questionnaire to all 50 states, the District of Columbia, and Puerto Rico. Three years later, a follow-up telephone survey was conducted. In addition, OTA sampled state CCH use in an urban area in each of three states. The CCH systems in these states were relatively more advanced than many state systems. *Id.*

60. *Id.* at 93-94.

61. *Id.* at 99.

the three state CCH systems sampled were 58%, 61%, and 85%.[62]

Professor Laudon found that the results of the three state CCH systems paralleled the findings at the federal level. He found that the percentage of records which were accurate, complete, and unambiguous was as follows: 12.2% of records disseminated from the Southeastern state; 18.9% of records from the Western state; and 49.4% of records from the Midwestern state.[63] Thus, even among states with more advanced computerized systems, there is a significant variance in data accuracy. Furthermore, "regardless of which state is examined, it would appear fair to conclude that data quality problems in state systems are far larger than is commonly known and more significant than heretofore imagined."[64]

Finally, the variations among states' laws, regulations, and procedures regarding criminal history data cannot be ignored in evaluating the III design. These laws control many facets of the state information systems on which III relies. They range from broad guidelines to specific requirements. Differences occur in the types of information that are maintained, dissemination regulations, provisions for individuals to challenge and review their records, utilization of verification and audit procedures to insure data accuracy, and court disposition monitoring.[65] Obviously, differences are exacerbated by the fact that only twenty-nine states maintain computerized systems. Variations in state record quality and in state laws "may complicate efforts to protect privacy and security of criminal history records . . . , [and] will result in nonuniform record content . . . unless nationwide standards are established."[66]

There are two main advantages to the III design. First, states have greater control over the dissemination of the records they create. Second, "III has the potential to speed up record exchange and reduce record duplication when fully implemented."[67] These improvements would be achieved presumably because there are many more state records than federal records and, under the III design, state records are maintained only at the state level and are not transmitted to NCIC.

---

62. *Id.* at 94. *See also* statistics cited *supra* note 44.

63. Laudon, *supra* note 20, at 21.

64. *Id.* at 22.

65. *See* OTA REPORT, *supra* note 6, at 99-105; *see also id.* at 72-73 (tables 13, 14, categorizing state laws and illustrating the number of states that have enacted each category).

66. *Hearings*, *supra* note 10, at 13 (statement of Fred B. Wood).

67. *Id.* Slow record exchange and record duplication is exacerbated by the fact that 30.4% of serious offenders have criminal records in more than one state. Of these multi-state offenders, 56% have records in two states, 16% in three states, 14% in four states, and 14% in five or more states. Furthermore, 75% of the multi-state offenders have records in at least one non-contiguous state. *Id.* at 53-54.

III. POTENTIAL FOR ABUSE AND VIOLATION OF INDIVIDUAL CONSTITUTIONAL RIGHTS

The extent of data inaccuracies in the NCIC system justifies the conclusion that current policies and procedures to insure data accuracy are inadequate and/or unenforced. While the FBI denies ultimate responsibility for data accuracy,[68] it imposes and suggests procedures to insure data accuracy that it does not (or cannot) enforce. This Note argues that these data inaccuracies violate individual constitutional rights, and prevent NCIC from operating efficiently and achieving its goals. The use or dissemination[69] of inaccurate WPF and CCH data violates the constitutional prohibition against denial of liberty without due process, and infringes on the right to privacy. Furthermore, the use and dissemination of inaccurate CCH data also denies the presumption of innocence, and violates the right to equal protection under the laws. Each of these constitutional harms will be discussed in turn.

A. Denial of Liberty Without Due Process

1. *The WPF*

Traditional procedural due process analysis first asks whether an individual has been denied life, liberty, or property. If so, the analysis asks whether the process which denied life, liberty, or property was adequate. A determination of the adequacy of the process involves consideration of the concepts of fundamental fairness and the opportunity to be heard. Due process promotes these intrinsic values, and is necessary to assure the correctness of decisions denying life, liberty, or property. It is obvious that a detention or arrest denies the individual his or her liberty. Thus, whether the use of inaccurate data, which leads to arrests of innocent people, constitutes a denial of due process turns on the adequacy of the process.

Generally, arrests do not violate due process if there is probable cause to make the arrest. When probable cause exists, the state has a reason to detain or arrest the individual. Probable cause is found when an officer of reasonable caution believes that an offense has been or is being committed. Such a belief is based on the facts and circumstances within his knowledge and of which he has reasonably trustworthy in-

---

68. *See supra* text accompanying note 20.

69. The use or dissemination of inaccurate data is clearly within the scope of the arguments presented here. The author does not argue, however, that the mere existence of inaccurate data violates constitutional rights. No doubt, as long as such data is in the system, an individual is "a 'marked man' . . . [and] continue[s] in this status into the indefinite future." United States v. Mackey, 387 F. Supp. 1121, 1124 (D. Nev. 1975). If the inaccurate data are never used, however, constitutional harm may not occur.

formation.[70] "The essence of 'probable cause' is a reasonable ground for a belief of guilt . . . ."[71] The existence of probable cause, which promotes the state interest of enforcing the criminal law, justifies the detention or arrest, and outweighs the assertion of due process rights.

Some courts have held that an NCIC hit alone constitutes probable cause.[72] The issue is far from clear, however,[73] and it is FBI and NCIC policy that a WPF hit alone is not probable cause for arrest.[74] Furthermore, as Professor LaFave points out:

> The point is *not* that probable cause is lacking because it turned out the "facts" upon which the officer acted were actually not true, for quite clearly information sufficient to establish probable cause is not defeated by an after-the-fact showing that this information was false . . . . *Rather, the point is that the police may not rely upon incorrect or incomplete information when they are at fault in permitting the records to remain uncorrected.*[75]

NCIC queries are made millions of times each year, almost all to the WPF and three other "hot files."[76] The number of invalid warrants in the WPF file creates an enormous potential for the arrest or detention of innocent people. When warrants fail to contain sufficient identifying information, more than one person is likely to be considered the subject of the warrant. This is particularly true when the wanted person has a common name. Finally, courts may overturn arrests based on

---

70. *See, e.g.*, Brinegar v. United States, 338 U.S. 160, 175 (1949); United States v. Roper, 702 F.2d 984 (11th Cir. 1983); United States v. Allen, 629 F.2d 51, 55-56 (D.C. Cir. 1980); Jackson v. United States, 302 F.2d 194, 196-97 (D.C. Cir. 1962); State v. Kolb, 239 N.W.2d 815, 817 (N.D. 1976).

71. Paula v. State, 188 So.2d 388 (Fla. 1966) (quoting McGain v. State, 151 So.2d 841, 844 (Fla. 1963)).

72. *See, e.g.*, *Roper*, 702 F.2d at 984; United States v. McDonald, 606 F.2d 552 (5th Cir. 1979); United States v. Palmer, 536 F.2d 1278 (9th Cir. 1976); Childress v. United States, 381 A.2d 614 (D.C. 1977); Patterson v. United States, 301 A.2d 67 (D.C. 1973); Commonwealth v. Riley, 284 Pa. Super. 280, 425 A.2d 813 (Super. Ct. 1981).

73. *See, e.g.*, People v. Ramirez, 34 Cal. 3d 541, 668 P.2d 761, 194 Cal. Rptr. 454 (1983); People v. Jennings, 54 N.Y.2d 518, 430 N.E.2d 1282, 446 N.Y.S.2d 229 (1981); People v. Lemmons, 49 A.D.2d 639, 370 N.Y.S.2d 243 (App. Div. 1975), *aff'd*, 40 N.Y.2d 505, 354 N.E.2d 836, 387 N.Y.S.2d 97 (1976); People v. Jones, 110 Misc. 2d 875, 443 N.Y.S.2d 298 (N.Y. City Crim. Ct. 1981).

74. *See* Manual, *supra* note 1, at Intro-2; *see also Probable Cause*, *supra* note 20, at 507; FBI, U.S. Dep't of Justice, Timeliness, Accuracy, and Probable Cause, NCIC Newsletter 5 (Winter 1984) ("It has been emphasized that an NCIC hit alone does not furnish probable cause to arrest.").

75. 1 W. LAFAVE, SEARCH AND SEIZURE § 3.5(c), at 636 (1978) (emphasis added). For a discussion of why an NCIC hit should not constitute probable cause, see *Probable Cause*, *supra* note 20. This Note will not argue that a hit is or is not a sufficient basis for probable cause; rather, it will focus on the existence of inaccurate data and police reliance on that data.

76. *See supra* note 24 and accompanying text.

originally valid, but subsequently cleared, warrants because due process rights were violated.[77] These are situations where the police rely on inaccurate data which exists because of police errors, and these data are used in violation of individuals' due process rights.

The FBI has instituted procedures to minimize the risks of wrongful arrests of innocent people, but the procedures are inadequate to protect due process rights. The key procedure is the confirmation policy for WPF hits.[78] If the procedure were followed and contact with the originating agency made, the confirmation policy would prevent a substantial number of arrests. It is clear, however, that the procedure is not always followed,[79] and there are cases where the originating agency cannot be reached.[80]

The inadequacy of current policies and procedures is also illustrated in the following scenario. A valid warrant leads to the arrest of the proper individual, but the person previously has cleared or vacated the warrant. Because the warrant was not removed from the system, the subsequent arrest of the same person on new charges may violate due process. The courts are divided on this issue; the result turns in part on the length of time the cleared warrant has remained in the system.

An example of a subsequent arrest being overturned is *United States v. Mackey*.[81] Defendant was stopped by the police on October 24, 1974, while hitchhiking, and was asked to produce identification. The officers made an NCIC query[82] which resulted in a hit for a probation violation. Despite defendant's protest that he had satisfied the warrant the previous May, he was arrested.

---

77. *See infra* text accompanying notes 81-90.

78. "Confirming the hit means to verify with the [originating agency] that the subject of the inquiry is identical to the subject in the record received, if the warrant is still outstanding, and whether or not the individual will be extradited. Upon receipt of a hit confirmation request, the originating agency must, within ten minutes, furnish a substantive response, i.e., a positive or negative confirmation or notice of the specific amount of time necessary to confirm or reject." User Agreement, *supra* note 3, at 5. *See also* Manual, *supra* note 1, at Intro-6, 7-19 to 7-20.

79. In all incidents concerning the named plaintiffs in Smith v. Gates, the police failed to confirm the outstanding warrants even though all necessary records were within the Sheriff's Department files or readily accessible. Complaint, *supra* note 34, paras. 2(d), 11, 18, 26, 31(g).

80. *See, e.g.*, United States v. Mackey, 387 F. Supp. 1121 (D. Nev. 1975); People v. Jennings, 54 N.Y.2d 518, 430 N.E.2d 1282, 446 N.Y.S.2d 229 (1981).

81. 387 F. Supp. 1121.

82. Although the opinion states that the officers had made an NCIC query, that apparently is incorrect. After the opinion was reported, the FBI told the presiding judge that the hit was made through CLETS, a California counterpart to NCIC. *Garbage In, Gospel Out*, *supra* note 2, at 511 n.13. This error, however, has no impact on the court's decision. *Id.* at 514 n.18.

During the booking process for the probation violation, the officers found an unregistered weapon. As a result, defendant also was booked on federal charges. Although the officers had tried to verify by telephone defendant's contention that the warrant was satisfied, they were unsuccessful. The officers then followed the usual procedure of verifying the warrant by teletype. This process confirmed defendant's contention, and the charge for the probation violation was dropped. The federal charge for possession of the weapon, however, was prosecuted.[83]

Defendant moved to suppress evidence, the shotgun, contending that the NCIC data were inaccurate and the arrest was, therefore, illegal. At the hearing on the motion, the police testified that defendant would not have been arrested if the NCIC query had not resulted in a hit. The *Mackey* court granted defendant's motion, stating:

> [T]he government's action was equivalent to an arbitrary arrest, and . . . *an arrest on this basis deprived defendant of his liberty without due process of law* . . . . Once the warrant was satisfied, five months before defendant's arrest, *there no longer existed any basis for his detention*, and the Government may not now profit by its own lack of responsibility."[84]

Mackey also establishes that NCIC policies on validation of warrants by originating agencies and Control Terminal Agencies are inadequate.[85] The FBI sends list of records to be validated every six months. The Control Terminal Officer in each state has seventy-five days to certify that the records are accurate and current.[86] Thus, even if FBI procedures are followed, an invalid warrant can exist in the system for more than eight months. Yet the *Mackey* court overturned an arrest based on a warrant that had been invalid for only five months.

Childress v. United States[87] illustrates the importance of the length of time that the invalid warrant remains in the system. In *Childress*, police officers observed defendant and a friend looking into parked cars and apparently casing a bank. The officers requested a "tag check" on defendant's car, which revealed four outstanding traffic warrants. The officers lost track of defendant's car until later in the day, when they saw the car and stopped it. The officers observed, in plain view, tools that could be used to break into cars, wire cutters, and a CB radio and

---

83. *Mackey*, 387 F. Supp. at 1121-22.

84. *Id.* at 1125 (footnote omitted) (emphasis added). Although the court based its holding on due process grounds, it noted the possibility of basing the decision on the fourth amendment. The court did not, however, find it necessary to pursue that basis. *Id.* n.9.

85. "Validation . . . obliges the [originating agency] to confirm the record is complete, accurate, and still outstanding or active." User Agreement, *supra* note 3, at 4.

86. Manual, *supra* note 1, at Intro-27; User Agreement, *supra* note 3, at 7-8; OTA REPORT, *supra* note 6, at 192.

87. 381 A.2d 614 (D.C. 1977).

tape player with cut wires. In addition, defendant voluntarily opened his trunk, which contained an apparently stolen CB radio.[88] He was ultimately found guilty of three counts of petit larceny and one count of destruction of property.

On appeal, defendant challenged his arrest and the evidence seized on the ground that there was no basis for the arrest because he had posted collateral for the outstanding traffic warrants four days prior to the arrest. The court upheld the arrest. It found that the warrant was originally valid, and that "[a]dministrative delays attendant to the operation of any metropolitan area police department resulted in failure to remove the satisfied warrants from the computerized 'active' list . . . ."[89] In a footnote, the court distinguished *Mackey* on the basis of "justifiable administrative delay," noting that two of the four days between posting the collateral and the arrest were a weekend.[90]

These cases illustrate the importance of accurate WPF data. Current NCIC policies are inadequate and permit inaccurate records to be used and disseminated. The use of these records leads to illegal arrests of innocent people, and violates the right to due process. Police officers treat these wrongfully arrested people like criminals, and often refuse to consider claims of innocence or mistaken identity until some later time.[91]

2. *The CCH File*

Violations of constitutional rights in the context of criminal history records were a concern long before NCIC began operations. Since 1924, the FBI has maintained the Identification Division ("Ident"), a manual fingerprint and criminal history data repository, pursuant to 28 U.S.C. § 534.[92] The development of NCIC has facilitated the use of criminal history records, and dissemination has been authorized to an increasing number of recipients, particularly those outside the public sector. The FBI does acknowledge that concerns about violations of constitutional rights exist; the regulations in 28 C.F.R. §§ 20.30-.38 concern the CCH file. Furthermore, the regulations are incorporated by reference into the User Agreement.[93]

---

88. *Id.* at 616.

89. *Id.* at 617.

90. *Id.* at 617 n.3.

91. *See supra* text accompanying notes 33-39; *see also supra* note 79.

92. Menard v. Mitchell, 328 F. Supp. 718, 720 (D.D.C. 1971).

93. User Agreement, *supra* note 3, at 2. In addition, the federal regulations and FBI policies concerning the CCH file apply to the III design as well. The NCIC Operating Manual includes the federal regulations in the section concerning III. Manual, *supra* note 1, at 10-1 to 10-5. The NCIC Advisory Policy Board also adopted a policy statement in December 1982 to make then-existing CCH policies apply to the III file. *Id.* at 10-6 to 10-

As was illustrated above, the data problems in CCH are the lack of disposition information; inaccurate disposition, charging, or sentencing information; and a lack of correspondence between the number of charges and dispositions.[94] If the recipient of CCH data is unaware of the distinctions between detentions, arrests, and convictions, and if CCH records do not make these distinctions sufficiently clear, there is substantial potential for violations of constitutional rights. Criminal justice officials, who are best able to comprehend the information in these records, tend to place less reliance on the data because it is inaccurate and incomplete.[95]

The dissemination and use of CCH data raises due process concerns. An arrest causes information to be placed in a CCH record. If charges are not pressed or exoneration occurs, the subject may not realize that the detention or arrest has been memorialized, or he may assume that the record will properly reflect the event. Even if the record is accurate, a recipient of the information may not understand the significance (or lack of significance) of the record. This is particularly true when CCH data are used to determine employment or licensing, in both the public and private sectors. As one court noted, "[t]he disabilities flowing from a record of arrest have been well documented: There is an undoubted 'social stigma' involved in an arrest record."[96]

In *Wisconsin v. Constantineau*,[97] the Supreme Court addressed the issue of the "social stigma" caused by activity falling short of a criminal conviction. Pursuant to a state statute, a local police chief caused a notice to be posted in all local liquor stores that sales of liquor to respondent were forbidden for one year.[98] The issue before the Court was "whether the label or characterization given a person by 'posting,' . . . is . . . such a stigma or badge of disgrace that procedural due process requires notice and an opportunity to be heard."[99]

The Supreme Court affirmed the ruling of the district court that the statute was unconstitutional:

> [C]ertainly where the State attaches "a badge of infamy" to the citizen, due process comes into play. "[T]he right to be heard before being condemned to suffer grievous loss of any kind, even though it may not involve the stigma and hardships of a criminal conviction, is a principle basic to our society."

---

22. Unlike CCH records, however, III records cannot be disseminated outside the criminal justice system pending completion of studies on this issue. *Id.* at 10-23 to 10-24.

94. *See supra* text accompanying notes 41-48.

95. *See supra* text accompanying notes 52-53.

96. Menard v. Saxbe, 498 F.2d 1017, 1024 (D.C. Cir. 1974) (footnote omitted).

97. 400 U.S. 433 (1971).

98. *Id.* at 434-35.

99. *Id.* at 436.

> Where a person's good name, reputation, honor, or integrity is at stake because of what the government is doing to him, notice and an opportunity to be heard are essential.[100]

Clearly, the state stigmatizes an individual when it permits dissemination of a CCH record. The dissemination of CCH data may occur without the individual's knowledge. Even if the person knows his criminal record will be disseminated, he may assume that it is accurate, or that the recipient will understand there was no conviction.

The Supreme Court held in *Paul v. Davis* that injury to individuals' reputations alone does not deny liberty.[101] But the Court did not overrule *Constantineau*; rather, it interpreted the language quoted above. The *Davis* Court said that liberty was denied when the government "significantly altered [Constantineau's] status as a matter of state law, and it was that alteration of legal status which, combined with the injury resulting from the defamation, justified the invocation of procedural safeguards."[102]

In *Constantineau*, the legal status that was altered was "the right to purchase or obtain liquor in common with the rest of the citizenry."[103] Here, the legal status at stake is the right of autonomy to pursue one's interests without being hampered by a baseless inference of criminal activity. These interests may include employment, education, a variety of government benefits, and many others.[104] Denial of these interests based on a false belief of a criminal record stigmatizes the individual. The denial of rights so fundamental to our society, coupled with the imposition of a social stigma, certainly requires procedural safeguards.

Other courts have raised the due process issue in connection with CCH. In *Utz v. Cullinane*,[105] appellants challenged the local police department's policy of routinely forwarding preconviction and postexoneration records to the FBI, which added the data to CCH. Appellants

---

100. *Id.* at 437 (citation omitted) (quoting Anti-Fascist Committee v. McGrath, 341 U.S. 123, 168 (Frankfurter, J., concurring)).

101. 424 U.S. 693 (1976).

102. *Id.* at 708-09.

103. *Id.* at 708.

104. "[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 by acquittal or complete exoneration of the charges involved." Menard v. Mitchell, 430 F.2d 486, 490 (D.C. Cir. 1970) (footnotes omitted). *See also* OTA REPORT, *supra* note 6, at 139-40; Tatum v. Rogers, 75 Civ. 2782 (CBM) (S.D.N.Y. Feb. 16, 1979) (findings of fact and conclusions of law), *reprinted in Hearings*, *supra* note 10, at 121.

105. 520 F.2d 467 (D.C. Cir. 1975).

contended that these records would inevitably be redisseminated nationwide to both public and private agencies. Appellants challenged the policy on several constitutional grounds: due process; right of privacy; and presumption of innocence.[106] The *Utz* court "agree[d] that there is a substantial bundle of constitutional rights which may be unnecessarily infringed when such arrest records are transmitted to the FBI with the knowledge that they will be retransmitted to a multitude of organizations for a multitude of purposes, all of which are susceptible of abuse."[107]

The *Utz* court explained in detail the ramifications—in due process terms—of dissemination of CCH data. The government contended that the utility of arrest records justified their maintenance.[108] The court disagreed, stating that the usefulness of the records for law enforcement "does not justify their dissemination for employment and licensing purposes."[109] The court noted further that "[w]hen arrest records are disseminated for law enforcement purposes, there are generally due process safeguards that should curtail most abuse."[110] The court doubted that safeguards were adequate to minimize abuse when records are disseminated for employment and licensing purposes.

Tarlton v. Saxbe[111] also discussed due process concerns where inaccurate criminal history records are disseminated. Appellant brought an action to expunge data of arrests which lacked disposition information, and arrests and convictions that he alleged were unconstitutional, from his criminal history record maintained in the FBI's manual Ident file.[112] On the issue of dissemination of inaccurate records, the *Tarlton* court held that 28 U.S.C. § 534 must be construed to prevent such disseminations, absent reasonable precautions to insure accuracy.[113] The court stated: "Dissemination 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 . . . . [It is] tantamount to permission to accuse individuals of criminal conduct without ever providing such individuals an opportunity to disprove that accusation."[114] Despite this comment,

106. *Id.* at 469-71.

107. *Id.* at 478. The court felt constrained to base its holding on statutory grounds, however, because a local ordinance prohibited the practices at issue. *Id.* at 469, 483-91.

108. More recently, prosecutors and district attorneys have indicated their dissatisfaction with criminal history records, and use them only as "pointers" to the location of more accurate data. *See supra* text accompanying notes 52-53.

109. *Utz*, 520 F.2d at 480.

110. *Id.* at 481 n.35.

111. 507 F.2d 1116 (D.C. Cir. 1974).

112. *Id.* at 1120.

113. *Id.* at 1122-23.

114. *Id.* at 1123 (footnote omitted).

however, the court clearly based its holding on its interpretation of 28 U.S.C. § 534, and not on constitutional grounds.[115]

The use of criminal history records within the criminal justice system itself can also violate due process.[116] In *Tatum v. Rogers*,[117] the court held that the New York Division of Criminal Justice Services, which maintained a state computerized criminal record system, had violated individuals' due process rights. The trial court found that records were so inaccurate that their use, particularly to set bail, violated constitutional rights.[118] The court noted that most criminal cases are resolved at the arraignment stage, at which time bail is set. Indigent defendants (plaintiffs in this case) are able to post only a minimal bail, and their defense lawyers have insufficient time to verify the accuracy of the computerized records. Yet, bail decisions are often made on the basis of inaccurate criminal history records, assuring that indigent defendants will be incarcerated until their cases come to trial.[119]

Fortunately, federal regulations have been promulgated which safeguard against due process violations. First, "[w]hen no active prosecution of the charge is known to be pending arrest data more than one year old will not be disseminated . . . *unless accompanied by information relating to the disposition of that arrest.*"[120] More importantly, the regulations provide individuals with a right of access to their CCH records. Individuals may review their record and request changes, corrections, or updates of the record by contacting the originating agency or the FBI, which will forward the request. If the originating agency changes the record, it must notify the FBI of the change, and the FBI will correct the record.[121]

Of course, the utility and effectiveness of these provisions depend on many factors. For example, people who are not aware that they can review their record will not do so. In addition, the procedure is rather involved, beginning with the fact that individuals must be fingerprinted again to identify them as the subject of the record.

One might also anticipate considerable delay before the process is complete. The delay may be caused not only by the time required to transmit requests between the various agencies involved, but also by the unwillingness of police departments to devote scarce resources to

---

115. *Id.* at 1124-25.

116. *See* Doernberg & Ziegler, *Due Process Versus Data Processing: An Analysis of Computerized Criminal History Information Systems*, 55 N.Y.U. L. REV. 1110 (1980).

117. 75 Civ. 2782 (CBM) (S.D.N.Y. Feb. 16, 1979) (findings of fact and conclusions of law), *reprinted in Hearings*, *supra* note 10, at 121.

118. *Id.* at 5-9, 13-14, *Hearings*, *supra* note 10, at 126-30, 134-35.

119. *Id.* at 13-14, *Hearings*, *supra* note 10, at 134-35.

120. 28 C.F.R. § 20.33(a)(3) (1985) (emphasis added).

121. *Id.* § 20.34. *See also* Manual, *supra* note 1, at 10-18 to 10-19, 10-25 to 10-26.

double-checking old cases. This is a particularly important problem because people may not check their records until they are aware that dissemination is about to occur. Finally, the success of these provisions also depends on the FBI's ability to enforce them.

The FBI does follow regulations which probably satisfy the "reasonable efforts" requirement mandated by the *Tarlton* court to help prevent inaccuracies. For example, for a state to participate in CCH, it must execute a User Agreement with the FBI, which subjects it to the NCIC policies and procedures.[122] The federal regulations also make clear the fact that responsibility for data accuracy rests on the originating agency.[123] Finally, failure to comply with the regulations can result in cancellation of access to the system.[124]

Of course, it has been shown that these regulations and procedures have not been completely effective; CCH data is far from 100% accurate.[125] Furthermore, the FBI rarely enforces the sanction available to it.

B. DENIAL OF THE RIGHT TO PRIVACY

1. *The WPF*

The right to privacy has been described in many ways. Access to information about individuals is often central to these definitions. Many commentators define the right of privacy in terms of information alone.[126] One author has defined privacy in terms of three interrelated components: the lack of information about an individual; the lack of attention paid to an individual; and the lack of physical access to an individual.[127] Thus, "[a] loss of privacy occurs as others obtain information

122. 28 C.F.R. § 20.36 (1985). *See also infra* text accompanying notes 161-87.

123. 28 C.F.R. § 20.37 (1985).

124. *Id.* § 20.38.

125. *See supra* text accompanying notes 41-48.

126. *See, e.g.*, A. WESTIN, PRIVACY AND FREEDOM 7 (1967) ("Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."); A. MILLER, THE ASSAULT ON PRIVACY 25 (1971) ("The basic attribute of an effective right of privacy is the individual's ability to control the circulation of information relating to him—a power that often is essential to maintaining social relationships and personal freedom.").

127. Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 428 (1980). "Attention is a primary way of acquiring information, and sometimes is essential to such acquisition, but attention alone will cause a loss of privacy even if no new information becomes known." *Id.* at 432. "Physical access here means physical proximity—that [another] is close enough to touch or observe [an individual] through normal use of his senses." Physical access can be more than another watching or listening to an individual, because the individual may not be aware that the other is watching or listening unless the other has physical access. *Id.* at 433.

about an individual, pay attention to him, or gain access to him."[128] In addition, the right to privacy is related to the values of individual liberty, autonomy, and creativity, and supports the ideal of a free and open society.

The initial inquiry, when a violation of the right to privacy is alleged, is whether the individual has a reasonable expectation of privacy.[129] This inquiry includes both subjective and objective elements. The court asks whether the individual has "exhibited an actual (subjective) expectation of privacy, and [whether] the expectation [is] one that society is prepared to recognize as 'reasonable.' "[130]

What are innocent individuals' expectations of privacy regarding arrests and criminal history information? Innocent people expect that the state will not detain or arrest them without reason. In addition, people expect that the government will not collect and collate information about them absent some sufficient government interest. Finally, when a sufficient state interest does exist, people expect the government to maintain accurate and complete information about them, so that those who use government data are not misled by the information.

The objective element of the right of privacy is illustrated by contrasting a valid arrest with an arrest based on inaccurate WPF data. An individual who is arrested pursuant to a valid warrant lacks a reasonable expectation of privacy. The state interest in protecting the public and enforcing the criminal law requires that the state have access to, and information about, individuals. Thus, although the individual may have a subjective expectation of privacy, society does not view this expectation as reasonable.

Innocent individuals, on the other hand, are denied the right of privacy when inaccurate or incomplete WPF data are disseminated and used. When an individual is arrested pursuant to an "ambiguous" warrant, one of two possible situations may exist. First, the arrest may be the result of a misidentification of the individual. As was shown above, misidentifications can be the result of a common name and a lack of sufficient identifying data in the warrant, or they may result from the unauthorized use of lost or stolen identification documents.[131]

In these situations, the arrested person is innocent; innocent people do not expect to be arrested absent a good reason. They do not expect the state to have access to them, particularly when the access is based on incomplete information about another person; nor do they expect to be forced to divulge information about themselves to the state. They

128. *Id.* at 428.

129. Smith v. Maryland, 442 U.S. 735, 740 (1979).

130. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

131. *See supra* text accompanying notes 33-39.

expect that the state will have sufficient data to identify correctly the subjects of its warrants.

The second situation involving inaccurate WPF data concerns people who were properly arrested in the past, but have subsequently cleared, vacated, or satisfied the arrest warrant. Because the warrant is no longer valid, the individual again has an expectation of privacy. These people may be constrained in some way—as, for example, by parole requirements—and the state may maintain the information about the person that was collected during the proper arrest. Absent additional wrongdoing, however, these people have a reasonable expectation that they will not be detained or arrested again, and that the information about them which the state maintains will be complete and accurate.[132]

Thus, when a person is arrested based on inaccurate WPF data, society views the expectation of privacy as reasonable. The state's interest in protecting the public and enforcing the criminal law is not served. At the same time, the state is interfering with the individual's life by detaining him and compelling him to divulge information without any reason to do so.

Furthermore, the right of privacy promotes other values and goals, which are indirectly harmed by the use of inaccurate WPF data. "[C]learly one of the important aspects of privacy [is] the way in which arguments for privacy are related to its function as a promoter of liberty."[133] The right of privacy limits government access to people and to information about them. As a result, the government's ability to interfere with individuals' lives is restricted. Thus, liberty is promoted.

The arrest or detention of an innocent individual pursuant to an invalid warrant is, as was shown above, a denial of liberty without due process of law. Because we respect innocent individuals' liberty in these circumstances, we should also respect their privacy interests, which promote that liberty. Governmental use and dissemination of information gathered in violation of the right of privacy can lead to the denial of liberty.

Finally, detentions or arrests place the stigma of criminal activity on individuals. As was shown above, the state cannot stigmatize individuals in this way without due process of law.[134] Where the arrests result from the use of inaccurate WPF data, not only are reputations harmed, but individuals are unfairly denied liberty and autonomy. In

132. State maintenance of complete and accurate information is crucial to the privacy right in terms of CCH data. *See infra* text accompanying notes 135-37.

133. Gavison, *supra* note 127, at 446 n.79.

134. *See supra* text accompanying notes 96-104.

addition, the stigma of criminal activity may be memorialized in government records such as the CCH file, leading to other harms.

2. *The CCH File*

The use of inaccurate CCH data may also violate the right of privacy. While it is true that an individual arrested pursuant to a valid warrant has no reasonable expectation of privacy, this loss of privacy is not without limit. Although the government may ultimately force the individual to divulge information and relinquish the right of privacy, it is important that the government not abuse the information it receives.

After an arrest, the expectation of privacy changes. Individuals may not be aware that the government maintains data about them.[135] Those who are aware expect that any information will be correct and complete. When it is not, the governmental use and dissemination of the inaccurate data denies the right of privacy in three basic ways.

First, the right of privacy is violated when the government creates a record and fails to keep it complete and up-to-date. The purpose of maintaining records is to disseminate them to others. When the government does so without the knowledge and permission of the subjects of the records, the privacy rights of those individuals are violated. Disseminating inaccurate information results in even greater harm, because the recipient acquires misleading information. Thus, the completeness and timeliness of CCH records are crucial. Yet the major problem with CCH record quality is the lack of disposition reporting.[136] When the government forces individuals to divulge information about themselves during arrests or criminal investigations, it cannot subsequently permit inaccurate information about those individuals to be provided to third parties.

Second, the right of privacy is invaded by the use and dissemination of inaccurate CCH data. When other criminal justice agencies receive the information, there is less of a threat to the right of privacy. The dissemination has occurred because the individual has been arrested again, or is involved in a subsequent stage of the criminal justice process such as sentencing or parole. Privacy concerns are raised, but individual rights may be adequately protected or outweighed by other interests. For example, CCH data are considered to be unreliable in the early stages of the criminal process, such as setting bail. These decisions occur soon after the arrest, when there is little time to confirm the accu-

135. The issue of whether maintenance of inaccurate data alone violates the right of privacy is not discussed here, although such maintenance may cause harm to individuals. Use and dissemination of inaccurate data leads to other harms which reflect violations of privacy rights more clearly.

136. *See supra* text accompanying notes 41-48.

racy of the CCH record. As a result, judges often refuse to consider incomplete or inaccurate CCH records when making these decisions, minimizing the threat to the privacy interest and the harm to the person. During later stages of the process, there is an opportunity to confirm the CCH record. When data are updated, complete, and accurate, they provide extremely valuable input in sentencing and parole decisions, outweighing privacy concerns.

CCH data are, however, also disseminated outside the criminal justice system to organizations in both the public and private sector. Individuals may not know that this dissemination occurs. Privacy concerns are greater in this case because of the loss of individual control over the information, and competing interests are less important than those in the criminal justice system. Because individuals have no control over the data, they must depend on the government to allow dissemination only to authorized recipients with valid uses for the information. Furthermore, individuals rely on the government to provide only accurate data. If the government disseminates inaccurate data, not only are recipients unable to use the data effectively, but also individuals may be subjected to other, more specific types of harm. For example, inaccurate data may harm individuals by denying education, licenses, and employment. While recipients may have a valid interest in knowing an applicant's criminal history, inaccurate data do not further this interest, because inaccurate data are not an indication of guilt.[137] Rather, the individual's expectation of privacy, based on the belief that the government will use and disseminate only accurate information, is denied.

In addition, values promoted by the right to privacy, such as liberty and autonomy, are impaired. A further goal of reintegrating criminals into society is hampered by allowing incorrect information to guide the decisions of potential employers and government agencies. Finally, as is illustrated in the next section, the presumption of innocence may also be denied.

C. Denial of the Presumption of Innocence

The dissemination of inaccurate or incomplete CCH data may violate the constitutional right to the presumption of innocence. "In our constitutional scheme, we operate under the salutary principle that an individual is presumed innocent of the charges of which he stands accused unless he is found guilty via a process replete with substantial procedural safeguards."[138] Numerous courts have held that an arrest record alone, without some showing of a conviction, is of no significance

137. *See infra* text accompanying notes 138-48.

138. Utz v. Cullinane, 520 F.2d 467, 478 (D.C. Cir. 1975) (footnote omitted).

on the issue of guilt.[139] Nevertheless, a record of a detention or arrest does inflict a stigma on an individual. Non-criminal justice agencies which receive CCH data may not understand that a detention or arrest alone is not an indication of misconduct.[140] The *Utz* court noted that "[e]ven if such records . . . were to include the actual disposition of the charges—and such dispositions frequently are not, in fact, included—the government knows that a derogatory inference will often nevertheless be drawn that the person who was arrested is also guilty of the crime charged."[141]

The *Utz* court and other courts have acknowledged that an arrest record causes difficulties for an individual seeking employment, licensing, or education. For example, one court expressed the belief that as long as potential employees who had not been arrested existed, it would be cheaper for an employer to disqualify automatically an applicant who had been arrested.[142]

A similar difficulty results if the recipient of CCH data cannot understand the record because of its cryptic form. The record at issue in *Menard v. Mitchell*[143] provides an excellent example of this problem. There, plaintiff had slept on a park bench for several hours, waiting for a friend to pick him up late one evening. When he awoke, he looked through the window of a rest home across the street to check the time. At approximately 3:00 a.m., two police officers questioned plaintiff about a report of a prowler near the rest home, and about a wallet belonging to another person that was apparently found on the ground near the bench. Plaintiff denied any knowledge of the wallet, and his friend, who arrived in the meantime, corroborated plaintiff's story. Nevertheless, the police arrested plaintiff and held him in custody for two days.[144]

---

139. *E.g.*, Schware v. Board of Bar Examiners, 353 U.S. 232, 241 (1957) ("When formal charges are not filed against the arrested person and he is released without trial, whatever probative force the arrest may have had is normally dissipated."); *Utz*, 520 F.2d at 478 ("An arrest record, without more, is a fact which is absolutely irrelevant to the question of an individual's guilt."); United States v. Dooley, 354 F. Supp. 75, 77 (E.D. Pa. 1973) ("[C]harges resulting in acquittal clearly have no legitimate significance. Likewise, other charges which the government fails or refuses to press or which it withdraws are entitled to no greater legitimacy."); Menard v. Mitchell, 328 F. Supp. 718, 724 (D.D.C. 1971) ("Under our system of criminal justice, only a conviction carries legal significance as to a person's involvement in criminal behavior.").

140. *See, e.g.*, Morrow v. District of Columbia, 417 F.2d 728, 741 (D.C. Cir. 1969) (there is a "likelihood that employers cannot or will not distinguish between arrests resulting in conviction and arrests which do not . . . .") (footnote omitted).

141. *Utz*, 520 F.2d at 479-80 (footnote omitted).

142. Menard v. Mitchell, 430 F.2d 486, 491 n.24 (D.C. Cir. 1970). *See also* Morrow v. District of Columbia, 417 F.2d 728 (D.C. Cir. 1969).

143. Menard v. Mitchell, 430 F.2d at 491.

144. Menard v. Saxbe, 498 F.2d 1017, 1019 (D.C. Cir. 1974).

No judicial hearing ever took place; the police released plaintiff after deciding that there was no basis to bring charges. The police did, however, transmit plaintiff's fingerprints and other information to the FBI's Ident division. After plaintiff filed suit to expunge his record, it was changed to state that the event was a not an arrest, but only a detention.[145]

Although the arrest record in the *Menard* case did not indicate a conviction, the record was clear that there had been an arrest, even though it was groundless and was later denominated a detention only. Most importantly, the record did not indicate where the "detention" took place, the circumstances of the incident, or even which state's laws were involved. This omission is particularly crucial because of the reference in the record to the section of the California Penal Code "849(b)(1)," which permits the police to release a suspect without bringing charges in circumstances such as these, and to deem the event a detention.[146]

A tension is created by the maintenance of CCH records which fail to reflect the fact that a detention did not result in a determination of guilt. On the one hand, the records provide relevant indicators about individuals. Potential employers want to know this information about a person who is seeking employment, particularly where a security clearance is necessary. Criminal justice agencies need the information if the person is involved in a subsequent incident. On the other hand, recipients may erroneously believe that the records indicate that the person was guilty of a crime. "Here, of course, we are relying primarily on the process being able to resolve the issue: did the person in fact commit the crime, and we are relying on the judgment of people to look at . . . the overall view of what the investigation shows."[147]

When the reason for the use of CCH records is subsequent criminal activity, the officials' expertise and the procedural safeguards of the process minimize the risk that the presumption of innocence will be de-

145. Menard v. Mitchell, 430 F.2d at 487. The CCH record read as follows:

> Date Arrested or Received—8-10-65
> Charge or Offense—459 PC Burglary
> Disposition or Sentence—8-12-65—Released—Unable to connect with any felony or misdemeanor at this time.
> Occupation—Student
> Residence of Person Fingerprinted—Saticoy & Canoga Canoga Park
>
> After the . . . complaint was filed, the entry under "Disposition or Sentence" was changed to read
> 8-12-65—Unable to connect with any felony or misdemeanor—in accordance with 849b(1)—not deemed an arrest but detention only.

Id. at 488 n.1.

146. *See id.* at 488-89.

147. *Hearings*, *supra* note 10, at 69 (statement of Kier T. Boyd).

nied. When the investigation is made by a non-criminal justice entity, however, to rely on the criminal justice process to protect the individual is a questionable practice. Any indication of criminal conduct is enough to make a candidate for employment or licensure undesirable. These recipients of CCH data do not understand the information they receive, and they have no guidance to help them utilize the data properly. It is too easy for recipients to assume that the individual was guilty of the crime, and to deny the employment or the license.

Whenever CCH data are used, regardless of the type of agency involved, the individual is forced to face the same criminal charge again. Within the criminal justice system, law enforcement officials draw whatever inferences seem appropriate from the arrest data; this can result in higher bail or a longer sentence. Individuals may not know that these investigations are occurring, and they have no opportunity to confront their accusers or present their own evidence.[148] These shortcomings amount to a denial of the presumption of innocence.

D. DENIAL OF EQUAL PROTECTION

Inaccurate CCH data which deny the presumption of innocence also deny equal protection under the laws. The equal protection clause requires that the government not improperly classify individuals. Furthermore, the equal protection clause guarantees that similarly situated people will be treated the same. Inaccurate CCH data classify innocent individuals as criminals, and place the innocent in the same category as the guilty. Thus, groups of individuals not similarly situated—the innocent and the guilty—are treated in the same way.

Statutory classifications which burden fundamental rights guaranteed by the Constitution have been subjected to strict judicial scrutiny, regardless of the characteristics of the burdened group. Fundamental rights include rights explicitly mandated by provisions of the Constitution which are distinct from the equal protection clause, such as the right of interstate migration.[149]

Many cases which have raised the issue of fundamental rights have concerned the right to "necessities," such as welfare and education. The Burger Court, however, has refused to expand the fundamental rights doctrine, holding that necessities are not fundamental rights.[150] The Court's position is that while these necessities are socially important, they are not expressly or impliedly guaranteed by the Constitution.[151] Although the Court has not expanded the list of fundamental rights, it

148. *Id.* at 95-96 (statement of Donald L. Doernberg).
149. *See, e.g.*, Shapiro v. Thompson, 394 U.S. 618 (1969).
150. San Antonio Indep. School Dist. v. Rodriquez, 411 U.S. 1 (1973).
151. *Id.* at 33-35.

has not abandoned the idea that fundamental rights are those rights expressly or impliedly guaranteed by the Constitution.

The issue of fundamental rights arises in the context of CCH data. This Note has demonstrated that rights guaranteed by the Constitution are burdened by the use and dissemination of inaccurate CCH data. Although a process, which may be legally adequate, does exist to correct errors, the use of inaccurate CCH data raises due process concerns.[152] More importantly, it has been shown that the use of inaccurate CCH data violates the right of privacy, which is guaranteed by the first, fourth, and other amendments.[153] Finally, it has been shown that such use denies the presumption of innocence, one of the most basic rights in our society.[154] It can therefore be argued that courts should apply the strict scrutiny standard to determine whether statutory and regulatory authority for the use and dissemination of CCH data are necessary to achieve compelling governmental interests.

Clearly, there are compelling governmental interests furthered by the use and dissemination of CCH data. It is questionable, however, whether the current statutory and regulatory scheme is necessary to achieve those goals. The "necessity" prong of the strict scrutiny test generally embraces the idea of less restrictive alternatives. If there are other ways for the government to achieve its compelling interests without causing harms, these methods must be used.

Despite the regulations in 28 C.F.R., CCH data are not accurate. As a result, not only are individuals harmed, but the criminal justice process is also made less efficient. Because the data are unreliable, prosecutors and judges cannot use the information to make decisions at various stages of the process, particularly to set bail.

If data quality were improved, both harm to individuals and systemic inefficiency would be minimized. Although CCH regulations are fairly complete, stricter requirements for disposition reporting are needed. Most importantly, the existing regulations should be enforced and compliance improved. Audits are one way to increase compliance with the regulations. In addition, current procedures to review CCH records and challenge their accuracy could be improved. These methods are less restrictive alternatives which would minimize the harm to individuals and better achieve governmental interests.

Equal protection claims are strongest where discriminatory, suspect classifications are drawn; this is particularly true when the classification is based on race. It cannot be argued that the current CCH statutory and regulatory scheme discriminates on the basic of race because there

152. *See supra* text accompanying notes 92-125.

153. *See supra* text accompanying notes 135-37.

154. *See supra* text accompanying notes 138-48.

is no legislative intent to discriminate. One court has, however, noted the racially discriminatory impact of arrest records in the context of employment decisions under Title VII of the Civil Rights Act.[155]

In *Gregory v. Litton Systems, Inc.*,[156] plaintiff had applied to defendant for employment. Defendant's employment questionnaire required applicants to reveal their arrest records. Plaintiff was not hired because he had been arrested fourteen times. This decision was based only on plaintiff's statement, and "not upon any consideration of convictions."[157]

Plaintiff sued pursuant to Title VII of the Civil Rights Act of 1964. Because Title VII is a remedial statute, "[h]istorical discrimination need not be shown in order to obtain relief from discrimination in fact, regardless of its cause or motive."[158] The district court found substantial evidence "that the apparently racially-neutral questionnaire actually operated to bar employment to black applicants in far greater proportion than to white applicants."[159] Accordingly, the questionnaire was invalidated because defendant failed to show any reasonable business practice for asking about arrest records.

In *Gregory*, the arrest record was supplied knowingly by plaintiff. Employment was denied based on that statement alone. An increasing number of employers are permitted to receive CCH arrest information about job applicants. Employers are likely to advance legitimate business purposes for the inquiry, thus defeating claims under Title VII. Therefore, it is most important that CCH data are accurate, so that correct employment decisions can be made.

Another equal protection concern arises from the disparity between state and federal laws regarding non-criminal justice access to CCH data. "These differences make it difficult to ensure equal protection under the law in the absence of national standards."[160]

IV. THE INADEQUACY OF CURRENT PROCEDURES

The serious data quality problems that exist in NCIC files, and the fact that these inaccuracies cause constitutional harms, demonstrate that current NCIC policies and procedures are inadequate. Although NCIC has only indirect statutory authority, comprehensive guidelines do exist for use of the WPF. Regarding CCH, federal regulations have been promulgated which, in theory, should minimize both data inaccu-

155. 42 U.S.C. § 2000e-5 (1982).
156. 316 F. Supp. 401 (C.D. Cal. 1970), *aff'd*, 472 F.2d 631 (9th Cir. 1972).
157. *Gregory*, 472 F.2d at 632.
158. *Id.*
159. *Id.*
160. *Hearings*, *supra* note 10, at 16 (statement of Fred B. Wood).

racies and constitutional violations. Yet many of these provisions have failed.

By reviewing the key procedures of the NCIC system, one can understand the relationships and divisions of responsibility among the FBI and local law enforcement agencies. It is the current status of these relationships and responsibilities which causes many of the problems with the WPF and CCH files. Another reason for the problems is the FBI's inability, or unwillingness, to enforce existing procedures.

Two FBI documents set forth the procedures for NCIC: the NCIC Operating Manual, and the NCIC User Agreement. The Operating Manual, which is distributed to all local law enforcement agencies that use NCIC, is analogous to an instruction booklet. It sets forth all policies, procedures, and regulations for the use of NCIC. The second document, the NCIC User Agreement, is a contract. When a state joins the NCIC system, the User Agreement creates a state agency, known as the NCIC Control Terminal Agency ("CTA"), which assumes responsibility for NCIC operations in that state. The purpose of the CTA is "to unify responsibility for system user discipline, and adherence to system procedures and policies within each state."[161] The CTA's responsibilities include providing hardware, software, funding, and training for all authorized users in the state. In addition, the CTA serves as a distribution center for other procedures and NCIC publications.[162]

Both the NCIC Operating Manual and the User Agreement define various requirements which are essential to WPF record accuracy. For example, they contain sections on "timeliness." The User Agreement emphasizes that timely entry of records insures maximum effectiveness. For a WPF file, a timely entry is one made as soon as a decision to arrest (or authorization to arrest) has been made, and the originating agency has determined that it will extradite the individual.[163] There are also guidelines for timely removal of records,[164] timely system queries,[165] and completeness of data.[166] Finally, "confirmation," a related procedure, is designed to insure that the subject of a hit is actually the

161. User Agreement, *supra* note 3, at 1.

162. *Id.* For a discussion of the additional procedures implemented by the CTA, see *infra* text accompanying notes 173-74.

163. Manual, *supra* note 1, at Intro-23; User Agreement, *supra* note 3, at 3.

164. "A timely removal from the file means an immediate removal once the originating agency has documentation the fugitive has been arrested or is no longer wanted." Manual, *supra* note 1, at Intro-24; User Agreement, *supra* note 3, at 3.

165. "Timely system inquiry means initiation of the transaction before an officer begins writing an arrest or citation document of any kind . . . ." Manual, *supra* note 1, at Intro-23; User Agreement, *supra* note 3, at 3.

166. "Complete records of any kind include all information that was available on the person or property at the time of entry . . . . Complete inquiries on persons include numbers that could be indexed in the record; i.e., Social Security, Passport, VIN, License

wanted person.[167]

Another User Agreement provision concerns "validation procedures."[168] The User Agreement restates that "[t]he primary responsibility for the entry and maintenance of accurate, timely, and complete records lies with the entering agency."[169] The FBI, aware that several courts have addressed the issue of responsibility for data accuracy,[170] warns in the User Agreement that "[i]t can be said that criminal justice agencies specifically have a duty to maintain records that are accurate, complete, and up to date."[171] Therefore, the User Agreement suggests that standards be employed that allow for accurate records and their dissemination.[172]

There is a second aspect to validation. Periodically, the FBI sends to each CTA a list of records it believes were entered by entities within the CTA's territory.[173] The CTA must certify to NCIC within seventy-five days that: the records have been reviewed; records that are not current have been removed and all remaining records are valid; and all records are complete and accurate. Failure to provide the certification within the specified time results in the purging of all records on the validation list by NCIC.[174] It is questionable whether these procedures are followed. Moreover, it has been shown that even when these validation procedures are followed there may be a denial of liberty without due process of law.[175]

NCIC's Advisory Policy Board is currently studying proposed changes to its validation procedures. The Board has approved the de-

---

Plates, Driver's License, etc. Inquiries should be made on all names/aliases used by the suspect." Manual, *supra* note 1, at Intro-24; User Agreement, *supra* note 3, at 4.

167. *See supra* text accompanying notes 78-80. *See also infra* text accompanying notes 218-19. Of course, it has been shown that these procedures are inadequate. Regarding timely entry of WPF records and the importance of the extradition decision, see Maney v. Ratcliff, 399 F. Supp. 760 (E.D. Wis. 1975). *See also* Extradition of Wanted Persons, *supra* note 6. Regarding timely removal of records, see, *e.g.*, United States v. Mackey, 387 F. Supp. 1121 (D. Nev. 1975); People v. Ramirez, 34 Cal. 3d 541, 668 P.2d 761, 194 Cal. Rptr. 454 (1983). Regarding complete records, see Complaint, *supra* note 34.

168. User Agreement, *supra* note 3, at 7-8. *See also* Manual, *supra* note 1, at Intro-27 to Intro-28.

169. User Agreement, *supra* note 3, at 6.

170. *E.g.*, Tarlton v. Saxbe, 507 F.2d 1116 (D.C. Cir. 1974); Menard v. Saxbe, 498 F.2d 1017 (D.C. Cir. 1974); Testa v. Winquist, 451 F. Supp. 388 (D.R.I. 1978); Maney v. Ratcliff, 399 F. Supp. 760 (E.D. Wis. 1975); People v. Ramirez, 34 Cal. 3d 541, 668 P.2d 761, 194 Cal. Rptr. 454 (1983).

171. User Agreement, *supra* note 3, at 7.

172. *Id.*

173. Manual, *supra* note 1, at Intro-27; User Agreement, *supra* note 3, at 7.

174. Manual, *supra* note 1, at Intro-27 to Intro-28; User Agreement, *supra* note 3, at 8.

175. *See* Burnham, *Computer Data Faulted in Suit Over Wrongful Arrest*, N.Y. Times, Jan. 19, 1986, § 1, at 11, cols. 2-5; *see also supra* text accompanying notes 81-86.

sign and implementation of a validation procedure which would automatically send on-line notices or requests for validation of records to the originating agency thirty days after entry, six months after entry, and annually thereafter. Validation would require the user to review the original entry and current supporting documents, and to consult with concerned parties, such as complainants, victims, prosecutors, and court personnel. System users would respond on-line within five days; failure to respond would cancel the record.[176]

The FBI also operates a Quality Assurance Program, which sends various types of error messages via NCIC to the originating agencies. One type, "non-serious" error messages, are generated by fingerprint records received by the FBI's Ident division. For example, a message is sent when Ident receives fingerprints identical with those of the subject of a WPF record from the same agency that entered the WPF record. NCIC will place a "locate" on the WPF record if it is not cleared, or its retention justified, within twenty-four hours. "Locates" generate "serious" error messages if the records are not cleared or cancelled within five days. On the fifth day, NCIC automatically suppresses these records, and purges them from the system shortly thereafter.[177]

The Operating Manual and User Agreement apply to the CCH file as well. In addition, federal regulations have been enacted which govern the use of CCH.[178] The regulations place the FBI in control of the CCH file,[179] and outline the types of offenses—generally serious or significant crimes—which are maintained in the system.[180] The regulations also provide that "[i]t shall be the responsibility of each criminal justice agency contributing data . . . to assure that information on individuals is kept complete, accurate and current . . . ."[181]

The regulations provide broad guidelines for dissemination of CCH

176. Quality Assurance Subcomm., NCIC Advisory Policy Board, Validation Improvement, *in* Report of Actions Taken at Sept. 18-19, 1984 Subcomm. Meeting 29 (1984), *reprinted in* NCIC Advisory Board Quality Assurance Subcomm. Meeting 1 (1984) [hereinafter cited as Subcomm. Report].

177. Report of Actions Taken at Sept. 18-19, 1984 Subcomm. Meeting 18-19 (Topic #8, Sanctions), *reprinted in* Subcomm. Report, *supra* note 176. NCIC sent approximately 4,400 non-serious error messages by teletype during 1983 and approximately 3,100 messages as of the date of the subcommittee meeting during 1984. These messages apparently concern only the WPF. Approximately another 6,000 messages were mailed during that same period; however, NCIC does not follow up on non-serious error messages that are mailed. Almost 50,000 serious error messages were sent during 1985, apparently concerning all NCIC files. In the first half of 1984, over 11,000 serious error messages were sent. *Id.* at 18-19, 23-26.

178. 28 C.F.R. §§ 20.30-.38 (1985).

179. *Id.* § 20.31.

180. *Id.* § 20.32.

181. *Id.* § 20.37.

data.[182] Records can be disseminated to criminal justice agencies,[183] to authorized federal agencies,[184] and to others, if authorized by federal or state statute and approved by the Attorney General, "for use in connection with licensing or local/state employment or for other uses . . . ."[185] Arrest data older than one year are not to be released unless the disposition of the arrest is included.[186] Finally, the regulations repeat the sanctions found in 28 U.S.C. § 534.[187]

To summarize, the FBI's role in maintaining CCH data quality is limited. The FBI passively receives data from local police agencies, stores the information in its computer, maintains the computer system, and facilitates the dissemination of the data. The FBI assumes no responsibility for the accuracy, completeness, or timeliness of the data; that responsibility is placed on the originating agency.

Furthermore, the FBI either cannot or will not enforce its procedures, including the federal regulations. The key enforcement provision, validation, is clearly inadequate. The high level of data inaccuracy in the CCH file makes it obvious that the FBI is not enforcing the federal regulations. Finally, the FBI rarely uses the only sanction available to it to enforce compliance with procedures.

Audit procedures are another means of achieving compliance with accuracy standards and other procedures. Audits insure accountability of government officials, establish public confidence in system operations, and facilitate improvements in data quality. Furthermore, audits are cost effective, because they are relatively inexpensive to implement, and lead to greatly increased system and management efficiency.[188] Audits are preferable to validations for verifying compliance because they are performed by an independent organization rather than the originating agency. They can be conducted on a random basis, providing an outside source of compliance which encourages originating agencies to maintain accuracy continuously.

Unfortunately, very few CTAs conduct audits, although the User Agreement suggests that this procedure be used. Only thirteen states

182. *Id.* § 20.33.

183. *Id.* § 20.33(a)(1).

184. *Id.* § 20.33(a)(2).

185. *Id.* § 20.33(a)(3). Under the current III program, however, records are disseminated only to criminal justice agencies. Manual, *supra* note 1, at 10-23 to 10-24.

186. 28 C.F.R. § 20.33(a)(3) (1985).

187. *Id.* § 20.33(b). *See supra* text accompanying note 16.

188. See NCIC, National Crime Information Center Control Terminal Agency Audit Manual 1 (1984) [hereinafter cited as Audit Manual]. The OTA Report estimated that five two-person audit teams could audit the 50 states, the District of Columbia, and Puerto Rico once per year. These teams could also audit the federal CCH records twice per year, as well as other small files. OTA Report, *supra* note 6, at 178.

have ever conducted an audit,[189] and only five states currently conduct audits on a regular basis.[190] The NCIC Advisory Policy Board has set a goal for all states to conduct audits beginning in January 1986; a more realistic time frame is January 1987.[191]

The FBI is testing and implementing the III file, an alternative to the CCH design,[192] in part as a response to the inadequacy of current procedures. Because federal regulations are not enforced and data quality is poor, states hesitate to contribute data to CCH, and several states have withdrawn as full participants.[193] Because state laws on dissemination vary greatly, and states lose control over the data contributed and received, the states have been opposed to the CCH file.

H.R. 896 is a bill which would establish a national computerized criminal history system based on the III decentralized design. It also seeks "[t]o improve State criminal justice information systems, including criminal history records; . . . [and] to ensure that criminal history records are accurate and complete . . . ."[194] The bill proposes to provide 100% funding through grants under the Omnibus Crime Control and Safe Streets Act of 1968[195] for states to establish criminal justice information systems.[196] This funding, however, is conditioned on compliance with the federal regulations within three years of receipt of the grant.[197] In addition, states must allow the Attorney General of the United States, or his designee, to audit the records at random to verify compliance with the regulations.[198]

Most importantly, the bill also limits dissemination of III data from the FBI to "departments and agencies . . . for criminal justice use."[199] This provision prevents the FBI from disseminating III for licensing or employment purposes. Of course, III contains actual criminal histories only on federal offenders; criminal histories of state offenders will be indexed only by name. The bill, however, prevents neither the dissemination of data on federal offenders in accordance with the federal regu-

189. OTA REPORT, *supra* note 6, at x.

190. Telephone interview with Fred H. Wynbrandt, Assistant Director, Criminal Identification and Information Branch, Division of Law Enforcement, California Department of Justice, and Chairman, NCIC Advisory Policy Board (Oct. 29, 1984).

191. *Id.*

192. *See supra* text accompanying notes 10-13, 58-67.

193. *See supra* text accompanying notes 50, 58-67.

194. H.R. 896, 99th Cong., 1st Sess., at intro. (1985).

195. 42 U.S.C. § 3741(b) (1982).

196. H.R. 896, *supra* note 194, § 3(b)(3).

197. *Id.* § 3(c)-4(a)(1).

198. *Id.* § 4(a)(2)-4(b).

199. *Id.* § 2(2). However, the recipient either must not have obtained III data in the previous three years, or, if it has received data, must have complied with the bill's provisions to insure data accuracy during the previous 180 days. *Id.*

lations, nor state dissemination of data from their own systems for any purpose. Thus, states will control whether, and to what extent, data will be disseminated.

This bill, if enacted, will reduce the inaccuracy of criminal history records and the resulting constitutional harms. Indications are, however, that the data quality of state criminal justice information systems is much worse than the present quality of CCH records.[200] Furthermore, although states may be more willing to participate in the III system because of greater control over the data, three important questions remain. First, in an era of severe budget cuts and high budget deficits, is it realistic for Congress to approve 100% funding for state systems, particularly when more than one third of the states do not have computerized systems? Second, will states want to establish their own systems with grant money that carries substantial "strings" concerning data quality? Finally, if the answer to both of these questions is no, will states want to establish their own computerized systems, and will state budgets be adequate to fund these projects?

Congressional legislation is clearly needed to improve the NCIC system. In this author's opinion, however, Congress has the power, and should accept the responsibility, to pass a much more detailed and comprehensive bill which establishes procedures for both the WPF and a national CCH system. Such a bill would allow NCIC to better fulfill its purposes and goals, insure higher data quality, and greatly minimize the risk of constitutional harm to individuals.

V. THE NEED FOR FEDERAL LEGISLATION

Current statutory, regulatory, and administrative procedures are inadequate to insure data accuracy. The arguments, cases, and studies of NCIC data accuracy discussed above demonstrate the problems and abuses that exist. FBI documents, policies, and procedures demand accuracy. Yet the FBI permits inaccurate data to exist and to be disseminated nationwide. The dissemination of inaccurate data not only infringes constitutional rights, but also impedes the administration of criminal justice and frustrates the achievement of NCIC's goals.

What is needed is a carefully drafted statute, setting forth these goals and policies and providing direct authority for NCIC. A statute can establish guidelines for the use and operation of the system, and set forth in detail the division of responsibility among criminal justice agencies to maintain data accuracy. It can provide incentives and sanctions to assure accuracy, and create an external agency to monitor compli-

200. *See supra* text accompanying notes 58-67.

ance. Finally, a statute can provide causes of action and remedies for individuals who are harmed by the use of inaccurate NCIC data.

The need for such an outside force is apparent. The current state of NCIC data indicates that the FBI alone cannot or will not maintain accuracy and enforce procedures. It is clear that the FBI should be responsible for enforcing NCIC procedures, and verifying compliance with them. Without random, independently conducted audits, and enforcement of sanctions for failure to comply, data accuracy is impossible to achieve.[201] A statute can provide for these measures.

Should the statute be enacted by state legislatures, or by the United States Congress? At least two courts[202] and others[203] have called for congressional action. There are several arguments which support the conclusion that Congress, rather than the states, should pass the required legislation.

The first issue to examine is whether Congress has the power to pass legislation in this area. Clearly, it does. Congress has already exercised some of this power, legislatively providing the current indirect authority for the NCIC system,[204] and establishing a specific NCIC file, the Missing Persons File.[205] In addition, a bill is now pending in Congress which would establish a national computerized criminal history

201. Telephone interview with Fred H. Wynbrandt, Assistant Director, Criminal Identification and Information Branch, Division of Law Enforcement, California Department of Justice, and Chairman, NCIC Advisory Policy Board (Oct. 29, 1984). The inadequacy of current compliance procedures is illustrated by the deposition testimony of a Lieutenant in the Boston Police Department. He stated that his department "did not follow the F.B.I.'s regulations requiring periodic checks that 'all records remaining in the system are valid and accurate.' " Burnham, *supra* note 175, col. 4.

202. Tarlton v. Saxbe, 507 F.2d 1116, 1131 (D.C. Cir. 1974) ("[W]e would welcome legislative action designed to meet the issues discussed in our opinion . . . . [T]he Congress is the appropriate institution to determine whether established . . . constitutional interests should be limited in service of other important social interests."); Menard v. Mitchell, 328 F. Supp. 718, 727 (D.D.C. 1971) ("The [FBI] 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. [footnote omitted]").

203. *E.g.*, OTA REPORT, *supra* note 6, at 138 ("Mandatory record quality standards, established by statute and backed up by the necessary funding and technical assistance to ensure implementation (and outside audit to ensure compliance), appear to be the most effective mechanism for protecting fifth, sixth, eighth, and 14th amendment rights."). For a broad discussion of national legislation, see *id.* at 153-88. *See also Hearings*, *supra* note 10, at 59 (statement of Fred B. Wood); *id.* at 97 (statement of Donald L. Doernberg).

204. 28 U.S.C. § 534 (1982).

205. Missing Children Act, Pub. L. No. 97-292, 96 Stat. 1259 (1982) (amending 28 U.S.C. § 534 (1982)). Although the NCIC Advisory Policy Board approved the Missing Person File on October 1, 1975, parents of missing children and other concerned individuals did not have access to the Missing Person File prior to passage of this Act. *The Missing Children Act*, 53 FBI L. ENFORCEMENT BULL. 17 (1984).

system based on the III design.[206] Furthermore, the federal regulations which exist concerning CCH were promulgated pursuant to a federal statute.[207] Congress in part derives this power to legislate from its spending power under the Constitution. Until 1984, federal funds were distributed to the states through LEAA block grants to develop computerized criminal justice information systems.[208]

Many states and localities, as well as others, have objected to national legislation on federalism grounds. Their argument is that crime, for the most part, is a matter of state concern. Furthermore, state or local agencies create NCIC records and have the responsibility for the accuracy and timeliness of those records. Therefore, states should maintain control over the dissemination of the records they create.

Although these concerns are important, they are not controlling. As shown above, Congress has the power to legislate in this area; Congress has indirectly placed the FBI in control of the NCIC system. In addition, the courts have made it clear that the FBI shares data quality responsibilities with other agencies. Furthermore, the NCIC system is essential for enforcing federal criminal law, and for effectuating the federal interest in controlling state offenders who cross state borders. Finally, state crime is increasingly viewed as an interstate problem requiring congressional concern and assistance because of the ease of mobility in our society.[209] For all of these reasons, federalism concerns should not preclude federal legislation in this area.

The scope of the NCIC system demands that it be controlled at the national level. Its very purpose is to make criminal justice information generated in one part of the country available to the rest of the country. If control is not uniform, or minimum standards are lacking, the usefulness and efficiency of the system will suffer. "[I]f Congress does not call the tune, then we have 50 different jurisdictions dancing to 50 different tunes. And unfortunately none of them are producing data of very reliable quality."[210]

It is unlikely that the states would pass uniform laws in this area. Criminal laws generally vary widely from state to state, as do laws concerning criminal justice information.[211] This diversity is consistent with the failure of states to enact uniform model laws proposed in the past, with the exception of the U.C.C. and a few others.

---

206. H.R. 896, *supra* note 194.

207. The regulations codified at 28 C.F.R. §§ 20.30-.38 were promulgated pursuant to 42 U.S.C. § 3789g (1982).

208. OTA REPORT, *supra* note 6, at 155.

209. *Id. See also, Hearings, supra* note 10, at 53-54 (statement of Fred B. Wood) (discussing percentages of offenders with records in more than one state).

210. *Hearings, supra* note 10, at 97 (statement of Donald L. Doernberg).

211. *See supra* note 65 and accompanying text.

Establishing a national system now may facilitate the implementation of technological advances throughout the system later. For example, at least two jurisdictions have instituted on-line court disposition reporting systems.[212] California now is implementing a computerized fingerprint identification system which will compare fingerprints of suspects to a data base of five million fingerprint records.[213] If a uniform computer system were established now, it would be easier to share this type of information in the future. Any potential communication problems between systems could be avoided.

Finally, national legislation is needed to define the proper uses of current files before new files are added. This protection is important because recent proposals for additional files have suggested using NCIC as an intelligence-gathering or surveillance tool.[214] Indeed, the most recent file, the Secret Service file, is being used in this manner with great success.[215] Fears that NCIC would be used in this way have been expressed from the beginning; the FBI has reassured the public that NCIC would not be a "Big Brother" type of system. While NCIC has demonstrated its usefulness for law enforcement, the fears remain. The current problems should be resolved before uses more threatening to constitutional rights are permitted.

VI. RECOMMENDED CONTENT OF FEDERAL LEGISLATION

National legislation should be comprehensive and detailed. Direct statutory authority for NCIC and all current files should be provided, and congressional approval should be required to add new files to the system. Guidelines for the content of records in the various files should be specified. Technical assistance and training should be available to CTAs and system users.

The FBI should continue to be the manager of the NCIC system, with responsibility for maintaining system hardware, software, and message switching equipment. The FBI currently has statutory author-

212. In Los Angeles, the Expanded Traffic Record System is in use. Court clerks can add, delete, and update records concerning traffic violations directly from terminals in their offices. Telephone interview with Byron R. Boeckman, Deputy City Attorney, City of Los Angeles (Nov. 20, 1984). These on-line disposition reporting systems can vastly improve criminal history data by improving the rate of disposition reporting. This was the experience in New York after it implemented an on-line disposition reporting system. *See* Tatum v. Rogers, 75 Civ. 2782 (CBM) (S.D.N.Y. Feb. 16, 1979) (findings of fact and conclusions of law 2-3), *reprinted in Hearings*, *supra* note 10, at 123-24.

213. Heffernan, *State Computer Will Speed Fingerprint Identification*, L.A. Times, Jan. 17, 1985, pt. I, at 3, col. 5. Recently, this new system aided in the arrest of two rape suspects. Harvey, *State's New Fingerprint Computer Nets Two Suspects in Rapes of Elderly Women*, L.A. Times, Jan. 4, 1986, pt. I, at 28, cols. 1-3.

214. *See supra* notes 1, 7 and accompanying text.

215. *See supra* note 7.

ity to collect criminal records, investigate federal criminal matters, and enforce the criminal law. FBI personnel helped develop NCIC, and are familiar with its operations. Allowing the agency to continue in its current role will provide consistency in NCIC operations, and avoid the expense of creating a separate agency.

Most importantly, Congress should define the FBI's responsibility for data accuracy. While all system users must bear partial responsibility for data accuracy—with originating agencies responsible for entering accurate data, updating records, and removing records that are no longer valid—the FBI must bear responsibility as the system manager to ensure compliance with accuracy requirements. Four procedures should be codified to enable the FBI to fulfill this obligation.

First, validation procedures should be revised. While the Advisory Policy Board validation proposal discussed above would improve data quality, validations must occur more frequently.[216] The statute should provide for an on-line system which requests validations one month after record entry, and every three months thereafter. This frequency of validations is necessary to adequately protect individuals' liberty, to ensure that records are complete and current, and to remove invalid or unnecessary records.

Second, the statute should provide for audits. NCIC has already done much of the groundwork for an audit system. An audit manual now exists which details the purposes and objectives of audits, auditor qualifications, exam standards, report requirements, methodology, and a series of questionnaires to be used before and during audits.[217] The requirements and procedures are quite detailed, and should be mandated by the statute, with two basic changes.

The first change concerns the agency which will conduct audits. If, as the FBI audit manual suggests, the FBI or CTAs were to conduct audits, the independence of the auditors and the value of the audits would be questionable. Because audits serve to insure that the system is properly operated, the FBI, as manager of the system, is not an appropriate auditor. Audits should be conducted by another agency such as the General Accounting Office, to provide a check on the FBI.

The second change concerns the use of pre-audit questionnaires. In order to be effective, audits should be regularly conducted on a random basis, without prior notification. Pre-audit questionnaires probably do provide useful information, and the FBI should be free to utilize them, but not as part of the audit process.

---

216. *See supra* text accompanying note 176. The need for frequent validations is obvious in light of the extended period for which WPF warrants are maintained. *See supra* text accompanying notes 31-32.

217. *See generally* Audit Manual, *supra* note 188.

The third procedure that should be codified in federal NCIC legislation is the ten minute confirmation procedure for WPF hits. The current procedure, which requires system users to confirm hits with originating agencies to verify that the right person is being arrested and is still wanted, is adequate. The problem arises in the areas of compliance and enforcement. Agencies that request confirmations and receive no response to their second request are directed to send a third request to the agency, with a copy to the FBI. As long as agencies actually do send these messages to the FBI, it should be possible to enforce the procedure.[218] The problem is that "there is no sanction that can presently be imposed for failure . . . to ensure compliance with the ten minute hit confirmation policy."[219] The statute should require, therefore, that third requests for confirmations routinely be sent to the FBI, and that sanctions be imposed on delinquent originating agencies. For example, the agencies could be prevented from receiving other NCIC data for a specified period of time.

Finally, the statute should mandate the use of NCIC's Quality Assurance Program, discussed above.[220] These provisions would improve compliance with NCIC procedures and provide a mechanism for their enforcement, leading to a significant improvement in data quality.

Regarding CCH data, specific guidelines for data dissemination should also be established by the legislation. Currently, disposition data must be provided within 120 days of record entry. The statute should supplement this requirement by providing that, if disposition data are unavailable, the CCH record should state the reasons for unavailability, and the date the data are expected to be available.[221] With this information, dissemination of the CCH record to criminal justice agencies would be permissible. CCH records without disposition data should not, however, be disseminated to non-criminal justice agencies for any reason. In addition, Congress should provide funds to state and local agencies to improve their operations and to implement technological advances, such as on-line disposition reporting and computerized fingerprint identification systems.[222]

Furthermore, the non-criminal justice agencies that will be permitted to receive CCH data should be specified. The current procedure, under which authorizations are provided by federal and state laws as

218. In 1983, the FBI received approximately 350 notices of failure to respond to second requests for confirmation. In the first half of 1984, the FBI received approximately 285 such notices. Subcomm. Report, *supra* note 176, at 27-28.

219. *Id.* at 20.

220. *See supra* text accompanying note 177.

221. For example, if a case is pending on appeal, the CCH record should reflect that fact.

222. *See supra* text accompanying notes 212-13.

well as the Attorney General, is inefficient. Congress should review the types of agencies which currently have access to CCH data, and add or delete agencies as it deems appropriate. These should be listed in the regulations.

Another procedure which should be included in the legislation is one which would assure individuals' right to review and challenge records. Existing federal regulations and NCIC procedures do provide for access to CCH and III data. To improve the effectiveness of the procedure, however, the regulations should provide a time frame within which the originating agency must respond to requests. In addition, an analogous procedure should be created for access to WPF data. In Los Angeles, a procedure has been instituted for individuals to obtain a "clearance document." It identifies and physically describes the individual, lists any warrants that have caused invalid detentions or arrests of the individual in the past, explains why he or she is not the wanted person, and states that no other warrants exist for the person.[223] This type of procedure should be available within the NCIC system, and arrestees or detainees should be so advised. It would minimize instances of innocent people being arrested repeatedly because they have a common name, or because a criminal is using their name as an alias.

Finally, there should be statutory authority for the NCIC Advisory Policy Board. The Board serves an important function because it is responsible for virtually all policy decisions and improvements in NCIC. Currently, the Board consists of law enforcement officers, prosecutors, and judges. The membership should be expanded in the near future to include defense representatives, such as public defenders, representatives from civil rights groups, like the American Civil Liberties Union, and interested citizens groups. This expanded Board should continue to develop and study proposals for improving NCIC, and work with Congress to promulgate and pass national NCIC legislation.

CONCLUSION

NCIC is a very useful tool for the administration of criminal justice. It collects and retrieves millions of pieces of information, and makes them available to any police department in the country. The system, however, can be no better than the information upon which it relies.

Data accuracy is a problem for NCIC. Inaccuracy subjects tens of thousands of individuals to the possibility of illegal detention or arrest in violation of their constitutional rights. Although some standards to insure data accuracy do exist, they are inadequate and underenforced. This state of affairs demands a solution that provides explicit authority

223. Smith v. Gates, Civil No. CA000619 (Cal. Super. Ct. (Los Angeles County) Sept. 4, 1984) (stipulated judgment and order granting permanent injunction paras. 19-24).

for NCIC, detailed procedures, effective means to enforce procedures and verify compliance, and higher data quality. The result will be protection of constitutional rights and increased system effectiveness.

The most viable solution to the problem of data accuracy is federal legislation. The NCIC system is already under the control of a federal agency. Congress has been active in this area before, and should step in now to regulate further the system. National legislation can establish guidelines for accuracy, methods for compliance, and assistance to achieve data accuracy. Standards which are uniform throughout the states will make the system easier to use and more efficient. A national bill which facilitates participation and cooperation between the states and the FBI will confirm the system's national scope, and better achieve the goal of nationwide assistance for law enforcement at all levels of government.

Mark A. Beskind