Fordham Urban Law Journal

Volume 10 | Number 3 Article 5

1982

Probable Cause Based on Inaccurate Computer Information: Taking Judicial Notice of NCIC Operating Policies and Procedures

Patrick Hand

PROBABLE CAUSE BASED ON INACCURATE COMPUTER INFORMATION: TAKING JUDICIAL NOTICE OF NCIC OPERATING POLICIES AND PROCEDURES

I. Introduction

Computer data banks increasingly have been used to supplement manual files as a means of storing criminal justice information. The most comprehensive computerized system is the National Crime Information Center (NCIC),[1] established in 1967.[2] It is managed by the Federal Bureau of Investigation,[3] but functions as a centralized computer bank for use by criminal justice agencies at the federal, state and local level.[4] Among other functions, the NCIC is used by police agencies as an investigative tool, assisting in the determination as to whether an arrest should be executed.[5]

---

1. In 1974, the NCIC was accessible to 5,000 criminal justice agencies, housed approximately 2.5 million records, and handled approximately 60,000 inquiries daily. De Weese, *Reforming Our "Record Prisons:" A Proposal for the Federal Regulation of Crime Data Banks*, 6 RUT.-CAM. L.J. 26, 30 n.20 (1974). Today, the NCIC is accessible to approximately 60,000 criminal justice agencies. Telephone conversation with Jeremiah J. Smith, Assistant Section Chief, National Crime Information Center (Jan. 7, 1982). By 1981 the NCIC housed approximately 9.2 million records, NATIONAL CRIME INFORMATION CENTER, U.S. DEP'T OF JUSTICE, NCIC NEWSLETTER 2 (Oct. 1981), and was handling approximately 300,000 transactions daily. *Departments of Commerce, Justice, and State, the Judiciary and Related Agencies Appropriations for* 1982: *Hearings Before a Subcomm. of the House Comm. on Appropriations*, 97th Cong., 1st Sess. 968 (1981) (statement of William Webster).

2. For a discussion of the origin and development of the NCIC, *see* De Weese, *Reforming Our "Record Prisons:" A Proposal for the Federal Regulation of Crime Data Banks*, 6 RUT.-CAM. L.J. 26 (1974).

3. The FBI manages the NCIC pursuant to authority given to the Attorney General's Office to "acquire, collect, classify, and preserve" criminal records for the official use of the federal government, the states, cities and other institutions, under 28 U.S.C. § 534(a) (1976), and delegated by the Attorney General under 28 C.F.R. § 0.85 (1980).

4. NCIC Operating Manual § 1.1, at Intro-1 (May 1, 1981). Examples of the state agencies comprising the NCIC are New York State Identification and Intelligence System (NYSIIS), California Justice Information System (CJIS), Law Enforcement Information Network (LEIN) (Michigan), Arizona Criminal Information Center (ACIC), and Florida Criminal Information Center (FCIC). The NCIC also includes control terminals at the city and metropolitan area level. *See generally* PROJECT SEARCH, INTERNATIONAL SYMPOSIUM ON CRIMINAL JUSTICE INFORMATION AND STATISTICS SYSTEMS (1974), which discusses state and regional criminal justice information systems.

5. The NCIC also is used to store criminal histories and to assist in the location of missing persons. NCIC Operating Manual § 1.1, at Intro-2. (Nov. 1, 1979).

The major advantage of computerized criminal information is that information is accessible to users nationwide.[6] Computerized information, however, is not necessarily more accurate than manual file systems, and because computer data bases increase accessibility, the effect of inaccuracies is magnified.[7] The use of computerized criminal information has raised important legal questions in cases where an arrest was made by a police officer relying on computer information which later proved to have been inaccurate at the time of the arrest.[8] If a search incident to an arrest based on unreasonably inaccurate information yields evidence of criminal activity, the defendant's fourth amendment guarantee against unreasonable search and seizure has been violated[9] and the evidence must be suppressed pursuant to the exclusionary rule.[10]

---

6. G. ZENK, PROJECT SEARCH: THE STRUGGLE FOR CONTROL OF CRIMINAL INFORMATION IN AMERICA 120 (1979).

7. *Id.*

8. The following cases invalidated arrests based on inaccurate computer information: United States v. Mackey, 387 F. Supp. 1121 (D. Nev. 1975); People v. Decuir, 84 Ill. App. 3d 531, 405 N.E.2d 891 (1980); People v. Lemmons, 49 A.D. 2d 639, 370 N.Y.S.2d 243 (3d Dep't 1975) (mem.), *aff'd on other grounds*, 40 N.Y.2d 505, 387 N.Y.S.2d 97, 354 N.E.2d 836 (1976); People v. Jones, 110 Misc. 2d 875, 443 N.Y.S.2d 298 (Crim. Ct. 1981). The following cases upheld arrests based on inaccurate computer information: Childress v. United States, 381 A.2d 614 (D.C. 1977); Patterson v. United States, 301 A.2d 67 (D.C. 1973); State v. Cross, 164 N.J. Super. 368, 396 A.2d 604 (App. Div. 1978); Commonwealth v. Riley, 425 A.2d 813 (Pa. Super. Ct. 1981). There is no published figure as to the extent of inaccurate information in the NCIC, but a recent random survey by the FBI Identification Division showed that a "large percentage" of apprehended fugitives had not been cancelled from the NCIC. NATIONAL CRIME INFORMATION CENTER, U.S. DEP'T OF JUSTICE, NCIC NEWSLETTER 2 (Sept. 1981).

9. The fourth amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation. . . ." U.S. CONST. amend. IV. The fourth amendment does not prohibit all warrantless searches and seizures, but requires that they not be unreasonable. Carroll v. United States, 267 U.S. 132, 147 (1925). The question of reasonableness depends upon whether the agency making the warrantless search or seizure has probable cause to believe that a crime has been committed, is in the process of being committed, or is about to be committed. Draper v. United States, 358 U.S. 307, 313 (1959). Probable cause is measured by the facts and circumstances within the knowledge of the arresting officer and of which the officer had reasonably trustworthy information. *Id.* Where probable cause standards are met, an arresting officer is entitled to make a full search of the arrestee's person. United States v. Robinson, 414 U.S. 218, 235 (1973), as well as the area within which the arrestee might gain possession of a weapon or destructible evidence, Chimel v. California, 395 U.S. 752, 763 (1969).

10. Mapp v. Ohio, 367 U.S. 643, 655 (1961); Weeks v. United States, 232 U.S. 383, 393 (1914).

This Note discusses the fourth amendment implications of arrest based on inaccurate computer information and articulates the circumstances under which such an arrest should be upheld.[11] NCIC safeguards are discussed and it is recommended that the courts take judicial notice of NCIC operating policies and procedures as a guide to determining whether probable cause has been established where an arrest is based on inaccurate computer information.

II. The Elements of Reasonable Action Pursuant to Inaccurate Computer Information

In *Whitely v. Warden*,[12] the United States Supreme Court set forth the "fellow officer" rule.[13] The Court held that police officers called upon to aid other officers in the execution of an arrest warrant are entitled to act on the strength of an official communication with the other officers, because the acting officers can assume that the communicating officers satisfied the probable cause requirement of the fourth amendment.[14] The arrest cannot stand, however, if the communicating officers do not have probable cause to send the communication.[15]

---

11. For a discussion of why an NCIC report can constitute probable cause to arrest, in addition to a discussion of NCIC history and procedures, *see Garbage In Gospel Out: Establishing Probable Cause Through Computerized Criminal Information Transmittals*, 28 HASTINGS L.J. 509 (1976). For a discussion of due process rights in regard to computerized criminal history records, *see* Doernberg and Ziegler, *Due Process Versus Data Processing: An Analysis of Computerized Criminal History Information Systems*, 55 N.Y.U. L. REV. 1110 (1980). *See also* A Symposium, *Computerized Justice Information Systems: A Recognition of Competing Interest*, 22 VILL. L. Rev. 1171 (1977); Note, *Extradition: Computer Technology and the Need to Provide Fugitives with Fourth Amendment Protection in Section 1983 Actions*, 65 MINN. L. REV. 892 (1981); N.Y. Times, Feb. 27, 1982, at 25, col. 2.

12. 401 U.S. 560 (1971).

13. *See W. La Fave*, 1 SEARCH AND SEIZURE § 3.5, at 623 (1978).

14. *Whitely*, 401 U.S. at 568. By holding that an arresting officer is entitled to act upon a communication with other officers, this probably has the effect of insulating the arresting officer from civil liability in an action for false arrest if it turns out that the fellow officers did not have probable cause to send the information. W. LA FAVE, 1 SEARCH AND SEIZURE § 3.5, at 623-24 (1978). In Blanchfield v. State, 104 Misc. 2d 21, 427 N.Y.S.2d 682 (N.Y. Ct. Cl. 1980), the claimant was imprisoned after being stopped by a police officer who had been advised that a computer printout showed that the claimant's license had been revoked. In fact, the license had been reinstated some days prior to the arrest. The claimant was incarcerated for more than a day until the police discovered that the license had been reinstated. *Id.* at 22-24, 427 N.Y.S.2d at 684-85. The claimant brought a successful tort action for false imprisonment, wherein the court ruled that the arresting officer did not have probable cause to make the traffic check. *Id.* at 28, 427 N.Y.S.2d at 687-88. *Accord* Testa v. Winquist, 451 F. Supp. 388, 392 (D. R.I. 1978).

15. *Whitely*, 401 U.S. at 568-69.

Where a defendant moves to suppress evidence seized incident to an arrest based on inaccurate computer information, the court should consider two issues, both emanating from *Whitely*, in deciding whether to grant the motion: first, whether the arresting officer acted reasonably pursuant to the information; and second, whether the agency that disseminated the information acted unreasonably in allowing the information to become inaccurate.[16] If both the arresting officer and the agency that sent the inaccurate information have acted reasonably, probable cause existed and the arrest should be upheld despite the inaccuracy.[17] The fourth amendment allows room for police mistakes, as long as they are errors "of reasonable men, acting on facts leading sensibly to their conclusions of probability."[18] In addition, the fourth amendment does not require a standard of certainty,[19] but requires that a source of information be reliable.[20] Finally, to invalidate an arrest solely because information relied upon in making the arrest later proves to be inaccurate, without a showing of unreasonableness on the part of the law enforcement agencies involved with the arrest, does not advance the deterrent purpose of the exclusionary rule.[21]

A. Police Officer Reliance

An arrest made pursuant to inaccurate computer information should not be invalidated on account of the actions of the arresting officer, unless the officer acted unreasonably in relying on the information. Probable cause must be measured by the facts known by the officer at the time of the arrest, without inquiry as to facts later discovered.[22] A subsequent discovery that computer information relied upon in making an arrest was inaccurate at the time of the arrest

---

16. *See* People v. Jones, 110 Misc. 2d 875, 443 N.Y.S.2d 298 (N.Y. Crim. Ct. 1981) (arrest invalidated where both the arresting officer and sending agency acted unreasonably), notes 25-28, 39-42 *infra* and accompanying text.

17. *See* Childress v. United States, 381 A.2d 614, 617 (D.C. 1977) (arrest was upheld where arresting officer acted reasonably and the NCIC information was only four days out of date), notes 47, 48 *infra*.

18. Brinegar v. United States, 338 U.S. 160, 176 (1948).

19. *See* Hill v. California, 401 U.S. 797, 803-04 (1971).

20. Aguilar v. Texas, 378 U.S. 108, 114 (1963).

21. United States v. Calandra, 414 U.S. 338, 348 (1974). "The [exclusionary] rule is a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a personal constitutional right of the party aggrieved." *Id.* (footnotes omitted). *See also* Childress v. United States, 381 A.2d 614, 617 (D.C. 1977).

22. *See* People v. Honore, 2 Cal. App. 3d 295, 300, 82 Cal. Rptr. 639, 642 (1969); Patterson v. United States, 301 A.2d 67, 69 (D.C. 1973); Commonwealth v.

does not render unreasonable the actions of the police officer at the time he relied on the information.

In addition, the *Whitely* "fellow officer" rule permits a police officer to rely on information supplied to him through an official communication.[23] This rule has been extended to communications using NCIC information and, therefore, the NCIC is a reliable source for purposes of the fourth amendment, when such information is supported by other facts and circumstances.[24]

A police officer cannot, however, unreasonably rely on computer information. In *People v. Jones*,[25] the defendant was arrested after officers received an "alarm" from their mobile field computer that the vehicle in which the defendant was a passenger had been reported as stolen. A search incident to the arrest revealed drugs, but the alarm later proved to be erroneous. At the trial on the drug charge, the arresting officer testified that, in his experience, almost 20% of all alarms turned out to be erroneous.[26] The court found this inaccuracy rate to be "unquestionably substantial" and unreasonable.[27] Therefore, the arrest was struck down because probable cause was not found to have existed at the time of the arrest.[28] Where the officer's prior experiences with computer information should lead him to believe that the computer source is not reliable and the officer does not make further inquiry as to the accuracy of the report, an arrest based on inaccurate computer information must be invalidated.[29] In addition, the courts should determine whether the arresting officer complied with the NCIC policy regarding verification.[30]

Riley, 425 A.2d 813, 816 (Pa. Super. Ct. 1981). *See also* Michigan v. DeFillipo, 443 U.S. 31, 37 (1979) (the fact that the statute under which the police officer made an arrest in good faith reliance was later ruled to be unconstitutional did not vitiate the probable cause that existed at the time of the arrest).

23. *Whitely*, 401 U.S. at 568.

24. *See* United States v. Davis, 568 F.2d 514, 516 (6th Cir. 1978) (an NCIC identification of a vehicle is sufficient to establish probable cause for the arrest of the one in possession of the vehicle); Daniels v. State, 276 So. 2d 441, 446-47 (Ala. 1973) (the fact that police had a report from the NCIC that a vehicle was stolen supplied probable cause to arrest the driver).

25. 110 Misc. 2d 875, 443 N.Y.S.2d 298 (N.Y. Crim. Ct. 1981).

26. *Id.* at 876, N.Y.S.2d at 299.

27. *Id.* at 884, N.Y.S.2d at 304.

28. *Cf.* Patterson v. United States, 301 A.2d 67, 69 (D.C. 1973) (arresting officer testified that he had never known the police teletype to be wrong and, therefore, arrest based on inaccurate NCIC information transmitted over the teletype was upheld).

29. *See* 110 Misc. 2d at 884 n.4, 443 N.Y.S.2d at 304 n.4 (1981).

30. *See* notes 59-65 *infra* and accompanying text.

B. Sending Agency Action

If a court determines that an arresting officer has reasonably relied on inaccurate computer information, it also must evaluate the actions of the agency that furnished the information, and invalidate the arrest if the agency did not have probable cause to send the information.[31] This result is dictated by *Whitely v. Warden*, which extends the fourth amendment probable cause requirement to all police agencies involved with the arrest.[32]

In *People v. Decuir*,[33] the defendant was arrested by a police officer who had been furnished with NCIC information that there was a warrant outstanding for the defendant's arrest. The NCIC information, in fact, had been inaccurate for two months.[34] The court granted the defendant's motion to suppress evidence on a narcotics charge stemming from a search incident to the arrest.[35] Following *Whitely*, the court held that although the arresting officer acted reasonably, the arrest was invalid because there was no probable cause independent of the invalid warrant.[36] The *Decuir* result is correct in that the two month failure to cancel the NCIC information concerning the outdated warrant was unreasonable action on the part of the sending agency and could not be used to furnish probable cause. The *Decuir* court did not, however, base its decision on the unreasonable delay in cancellation, but instead interpreted *Whitely* as meaning that the fact that the warrant was no longer valid alone vitiated probable cause. While this interpretation is technically correct, such a strict interpretation is unnecessary because the fourth amendment requires a standard of reasonableness, not certainty.[37] If certainty were required, any delay by a police agency in updating its computer records would be unreasonable and would result in the invalidation of an arrest made in reliance on the records.[38]

---

31. *See* People v. Decuir, 84 Ill. App. 3d 531, 532-33, 405 N.E.2d 891, 893 (1980).

32. *See generally* W. La Fave, 1 Search and Seizure § 3.5, at 623-24 (1978).

33. 84 Ill. App. 3d, 531, 405 N.E.2d 891 (1980).

34. *Id.* at 532, 405 N.E.2d at 892.

35. *Id.* at 533, 405 N.E.2d at 893.

36. *Id. Accord* People v. Lemmons, 49 A.D. 2d 639, 640, 370 N.Y.S.2d 243, 244-45 (3d Dep't 1975) (mem.), *aff'd on other grounds*, 40 N.Y.2d 505, 387 N.Y.S.2d 97, 354 N.E.2d 836 (1976).

37. *See* note 19 *supra* and accompanying text.

38. In some situations, the delay could be unavoidable, and not unreasonable. For example, a stolen car entered in the NCIC as stolen might be recovered on a weekend, in which case there could be a delay in cancellation of the entry until the beginning of the workweek, or an NCIC user terminal may be temporarily out of service.

The issue of delay in updating computer information was addressed by the court in *People v. Jones*,[39] where a three month failure on the part of the sending agency to correct computer information was held to be grounds for invalidating an arrest made in reliance on the information.[40] The court recognized, however, that "some delay is to be expected" in correcting or updating computer records and placed the burden of establishing that the delay is reasonable on the sending agency.[41]

The *Jones* decision correctly interpreted *Whitely* because it would allow an arrest based on inaccurate computer information to be upheld where the purpose of the exclusionary rule is not advanced by the suppression of evidence seized incident to the arrest. Under *Jones*, the sending agency must show that it did not act unreasonably in disseminating the inaccurate information.[42] Conversely, under *Decuir*, the actions of the sending agency are irrelevant because the mere fact that the computer information underlying the arrest was inaccurate would invalidate the arrest.[43] The *Decuir* rationale emphasizes form over substance where the inaccuracy is not the fault of the police. The *Jones* rationale, however, allows room for a "good faith" exception to the exclusionary rule.[44] Rather than requiring the invalidation of an arrest solely because the information relied on in making the arrest later proves to be inaccurate, *Whitely* should require that courts examine the actions of the agency to determine whether it acted unreasonably in allowing the information to become inaccurate.

---

39. 110 Misc. 2d 875, 443 N.Y.S.2d 298 (N.Y. Crim. Ct. 1981).

40. *Id.* at 884, 443 N.Y.S.2d at 304. The defendant had been the passenger in a car that was stopped by officers who had entered the car's license tag number into their mobile field computer and received an "alarm" that the vehicle had been reported as stolen. One of the officers radioed the police dispatcher and received confirmation that the vehicle was wanted. The officers stopped the vehicle in question and advised that driver that she was under arrest for possession of a stolen vehicle. The driver told the officer that the car was not stolen, but was borrowed. The officer called the dispatcher again and was again told that the car was reported as stolen. The driver and the other passengers were arrested. Controlled substances were subsequently seized from one of the passengers. The occupants of the car were then taken to the precinct station, where it was ascertained that although the vehicle had been stolen three months earlier, it had been recovered three days later and returned to its owner, and that the driver was using the car with the owner's permission. The driver was then released; her companions, however, including the defendant, were charged with drug offenses. *Id.* at 876-77, 433 N.Y.S.2d at 299-300.

41. *Id.* at 884, 433 N.Y.S.2d at 304.

42. *See* notes 39-41 *supra* and accompanying text.

43. *See* notes 33-37 *supra* and accompanying text.

44. *See, e.g.*, United States v. Williams, 622 F.2d 830 (5th Cir. 1980), *cert. denied*, 449 U.S. 1127 (1981).

The length of the delay in failing to update inaccurate computer information has been the determinative factor of several cases involving arrests based on inaccurate computer information. In *Patterson v. United States*,[45] for example, an arrest based on NCIC information was upheld despite the fact that "for some unexplained reason" the information had been inaccurate for fifteen hours prior to the arrest.[46] Similarly, in *Childress v. United States*,[47] the failure on the part of police to cancel information regarding warrants that the defendant had satisfied four days prior to the arrest was held to be a reasonable administrative delay.[48]

---

45. 301 A.2d 67 (D.C. 1973).

46. *Id.* at 69. The defendant had been stopped after police officers had noticed that the license tags on the vehicle he was driving were on their "stolen list". One of the officers radioed for an NCIC check, and the dispatcher replied that the vehicle was still wanted. In fact, the vehicle had been recovered some fifteen hours before the arrest, but the NCIC entry had not yet been cancelled. Relying on the inaccurate NCIC information, the officers arrested the defendant. The vehicle was searched and a loaded revolver was discovered. At some point, the defendant was cleared of suspicion of auto theft by establishing to the satisfaction of the officers that he was driving the vehicle with the owner's authorization, but he was charged with the weapons offenses. *Id.* at 68-69.

47. 381 A.2d 614 (D.C. 1977).

48. *Id.* at 617. Police officers observed the defendant acting in what the officers considered to be a suspicious manner. The officers watched the defendant get into an automobile, whereupon one of the officers radioed for a check on the tag numbers. The dispatcher responded that there were four traffic warrants outstanding for the defendant. The defendant actually had posted collateral for the warrants four days earlier, but the warrants had not been removed from the computerized list. Later, in reliance on the inaccurate computer information, police officers stopped the car and ordered the defendant to get out. The officers observed burglary tools and stolen property inside the car in plain view. Advising the defendant that he was being stopped because of the outstanding warrants, the police requested and received his permission to open the trunk, wherein they found more stolen property. The defendant was arrested and charged with petty larceny and destruction of property. *Id.* at 616. The court held that reasonable police reliance on misinformation produced by a reasonable delay "presents a situation in which [granting the defendant's motion to suppress] would do nothing to advance the purposes of the exclusionary rule." *Id.* at 617. *See also* Commonwealth v. Riley, 425 A.2d 813 (Pa. Super. Ct. 1981) (arrest based on NCIC information four days out of date was upheld); State v. Cross, 164 N.J. Super. 368, 396 A.2d 604 (App. Div. 1978). In *Cross*, the defendant was stopped by a state trooper for a speeding violation. The trooper radioed for an investigative check on the registration through the NCIC, and was informed that the vehicle was entered as stolen by the Camden Police Department. On the basis of this information, the defendant was arrested for possession of a stolen vehicle. The defendant insisted that he owned the vehicle and had reported it as stolen, but that it had since been returned to him. The trooper arrested the defendant after searching the glove compartment and finding drugs. Upon returning to the police station the trooper telephoned the Camden police to check the status of the vehicle, and he was informed that the defendant's assertions were correct. The Camden police admitted that "they forgot to cancel their teletype in the NCIC computer." At trial on the drug

An arrest based on computer information five months out of date was struck down in *United States v. Mackey*.[49] The court recognized the fourth amendment basis for the defendant's claim, but decided the case on due process grounds.[50] It held that the five month failure to cancel the information amounted to a "capricious disregard" of the defendant's due process rights,[51] in that the defendant was a "marked man" for five months prior to his arrest and had been subject to an unwarranted arrest at any time.[52] The court in *Mackey* may have been attempting to extend the broader range of protections afforded by due process to individuals arrested in the future pursuant to inaccurate computer information.[53] While the elasticity of due process is beneficial to the extent that it protects a defendant who has suffered an injustice not clearly definable under a specific provision of the United States Constitution, courts are not expected to formulate a rule of constitutional law broader than is necessary to fit the facts of the case.[54]

---

charge, the trooper testified that he believed the Camden police informed him that the vehicle had been reported as stolen five weeks before. *Id.* at 369-71, 396 A.2d at 604-05. The court held that the information supplied to the officers gave rise to probable cause to arrest, and that the search was valid as incident to a valid arrest. *Id.* at 372-73, 396 A.2d at 606. The *Cross* decision is questionable, in that the actions of both the arresting officer and the sending agency appear to have been unreasonable. The officer acted unreasonably in searching the defendant before receiving verification on the information, even while the defendant was insisting that it was incorrect. The admission by the sending agency that it had forgotten to cancel the NCIC information is a clear indication of unreasonableness, although the five week failure to cancel the information, by itself, should have been enough to vitiate probable cause.

49. 387 F. Supp. 1121 (D. Nev. 1975). The defendant was stopped and questioned by police who saw him unlawfully hitchhiking. He was arrested after the police radioed his name to their dispatcher and were informed that the computer showed a warrant outstanding for his arrest. Despite assertions by the defendant that the warrant was no longer valid, he was searched and an unregistered shotgun was found in his possession. Sometime afterward, the police received information that the defendant had complied with the warrant five months earlier. Nonetheless, the defendant was charged with the weapons offense. *Id.* at 1121.

50. *Id.* at 1125 n.9.

51. *Id.* at 1125.

52. *Id.* at 1124.

53. Unlike the fourth amendment, which sets a definite standard of reasonableness, due process "is far from mathematically precise: since due process is not a mechanical yardstick, it does not afford mechanical answers." B. SCHWARTZ, CONSTITUTIONAL LAW § 7.2, at 238 (2d ed. 1979). The Supreme Court has held that due process requires a standard of "fairness," Manson v. Brathwaite, 432 U.S. 98, 113 (1977), and has stated that due process means that "convictions cannot be brought about by methods that offend a sense of justice." Rochin v. California, 342 U.S. 165, 173 (1952).

54. Liverpool, N.Y. & Phil. S.S. Co. v. Commissioners of Emigration, 113 U.S. 33, 39 (1885).

Under the facts of *Mackey*, the defendant was afforded ample protection by the fourth amendment. The arrest should have been invalidated because the five month failure to cancel the information was unreasonable.[55] A due process analysis permits courts to apply a less specific standard than reasonableness and could discourage the use of computers as a law enforcement tool. Due process should not be utilized unless it appears that the fourth amendment does not adequately protect the public against false arrest pursuant to inaccurate computer information. The fact that subsequent cases involving arrest based on inaccurate computer information did not adopt the *Mackey* due process rationale, but instead used the fourth amendment, indicates that the courts have found the fourth amendment to afford adequate protection.[56]

The extent of the delay in updating computer information provides courts with an indicium of whether the sending agency acted reasonably. Where the delay is lengthy, for example, two months in *Decuir*, or five months in *Mackey*, the arrest should be invalidated without further inquiry. In cases where the delay is not manifestly unreasonable, courts should examine whether NCIC policies and procedures[57] have been followed in order to determine whether probable cause standards have been met.[58] Where the sending agency does not adhere to these policies and procedures, the arrest should be invalidated as violative of the fourth amendment.

---

55. *See* People v. Decuir, 84 Ill. App. 3d 531, 532-33, 405 N.E.2d 891, 892-93 (1980) (invalidating an arrest based on NCIC information two months out of date) People v. Jones, 110 Misc. 2d 875, 884, 443 N.Y.S.2d 298, 304 (N.Y. Crim. Ct. 1981) (invalidating an arrest based on computer information three months out of date).

56. *See* note 8 *supra*.

57. *See* Section III *infra*. The NCIC policies and procedures would not be applicable where the inaccurate information has not been entered into the NCIC, but is contained within the state system. Information cannot be entered into the NCIC by a user agency unless that agency is willing to extradite the individual. NCIC Operating Manual § 4.2.2, at Intro-63 (Nov. 1, 1981). The information, however, could be used within the state system. Although the NCIC policies and procedures would not apply, the fourth amendment issue would still be present. NCIC policy is recommended by the NCIC Advisory Policy Board, which is composed of 20 elected representatives from criminal justice agencies throughout the United States, and six members who are appointed by the Director of the FBI. *Id.* § 1.5, at Intro-5 (Aug. 1, 1979).

58. *But see* United States v. Caceres, 440 U.S. 741 (1979), which upheld the introduction into evidence of a tape recording made by an IRS agent, who had not obtained the proper authorizations required under IRS regulations for monitoring suspects, at the respondent's trial for bribery of an IRS agent. *Id.* at 743-44. The Court held that the IRS "was not required by the Constitution or by statute to adopt any particular procedures or rules before engaging in consensual monitoring and

III. Judicial Notice of NCIC Operating Policies and Procedures

NCIC operating policies and procedures relate to the actions of both the arresting officer and the sending agency. The courts should take judicial notice of these safeguards and base their decision of whether probable cause existed on the degree of compliance with them.

For purposes of providing individuals with adequate protection under the fourth amendment, the most important policy is one whereby an NCIC "hit" (an inquiry receiving an affirmative response)[59] alone, does not furnish probable cause to arrest.[60] The hit is only one factor which the officer must consider in conjunction with other circumstances before taking action.[61] The inquiring agency must communicate immediately with the originating agency to verify the accuracy of the hit.[62] This policy, known as "the ten minute rule,"[63] requires the originating agency to, within ten minutes of the communication, either confirm the accuracy of the hit, inform the inquiring agency that the record is no longer accurate, or give notice of the specific amount of time necessary to confirm or reject.[64]

The importance of the ten minute rule is that the NCIC has recognized the fourth amendment problems inherent in using computer information as an investigative tool and requires its user agencies to ensure that the information being relied on in making the arrest is accurate. According to this rule, an arresting officer can never assume NCIC information to be accurate until it is verified. Where the arresting officer does not make an immediate attempt to verify, probable cause has not been established and the arrest should be invalidated.

---

recording." *Id.* at 749. In the context of arrest, however, police are required by the fourth amendment to act reasonably, and it seems that *Caceres* can be distinguished from the computer cases on that ground.

59. For example, an individual is stopped by a police officer affiliated with an NCIC user department. The officer calls his dispatcher and gives the individual's name, or the vehicle identification number (VIN) of the vehicle he is driving. The department would then check the individual's name, or the VIN, through the NCIC. If the NCIC computer listed the individual as wanted, or the vehicle as reported stolen, the department would be informed of the "hit" through its terminal.

60. NCIC Operating Manual § 1.2, at Intro-2 (Nov. 1, 1979).

61. *Id.*

62. *Id.* § 1.7, at Intro-7a (Nov. 1, 1981).

63. Telephone conversation with Jeremiah J. Smith, Assistant Section Chief, NCIC (Jan. 7, 1982).

64. NCIC Operating Manual § 1.7, at Intro-7a (Nov. 1, 1981).

The NCIC is a voluntary system and a user agency need not make an entry into the system.[65] Once an agency enters a record into the NCIC, however, it is responsible for the accuracy, timeliness and completeness of the record.[66] The NCIC requires an agency acting on the basis of a record in the system to immediately enter a "locate" into the system to signify to the originating agency that the record acted upon is no longer needed in the system.[67] As soon as the locate is placed, the originating agency is required to cancel the record from the system. If it does not comply, the NCIC computer will remove the record five days later in the case of individuals, or ten days later in the case of stolen vehicles and property.[68] The courts should examine whether this procedure has been complied with in conjunction with the *Whitely* requirement that the law enforcement system as a whole adhere to the fourth amendment.[69] The failure to enter or respond to a locate should be treated as *prima facie* evidence of unreasonable conduct, even if the period between when the information should have been removed and the time of the arrest is brief.

Although the FBI does not assume responsibility for any NCIC records other than those which it enters into the system,[70] as manager of the system, the FBI attempts to ensure accuracy through several

---

65. An entry is a message placing a new record in an NCIC file by a user agency. NCIC Operating Manual § 2.2.1, at Intro-8. An agency might withhold information from the NCIC "because of criminal justice priorities, budgetary limitations, or other reasons determined to be legitimate by the state control terminal agency." *Id.* § 1.6, at Intro-6 (Nov. 1, 1981). User agencies cannot enter information about a wanted person into the NCIC unless the state is willing to extradite the individual. *Id.* § 4.2.2, at Intro-63 (Nov. 1, 1981).

66. NCIC Operating Manual § 1.3, at Intro-3 (May 1, 1981). In Testa v. Winquist, 451 F. Supp. 388 (D. R.I. 1978), plaintiffs sued police officers who had arrested them after receiving NCIC information that erroneously listed a vehicle in the possession of the arrestees as stolen. The court held that the plaintiffs could state a cause of action if they could show that the arresting officers unreasonably relied on the NCIC information and on the sending officer's confirmation, and that the administrator of the issuing NCIC agency had a duty to minimize the risk of false arrest by requiring that the records be constantly updated. *Id.* at 390-94.

67. Telephone conversation with David Nemecek, Section Chief, NCIC (Jan. 14, 1982).

68. *Id.*

69. *See* Section II, B. *supra.*

70. NCIC Operating Manual § 1.7, at Intro-7 (Nov. 1, 1981). *But see* United States v. Mackey, 387 F. Supp. 1121, 1123-24 (D. Nev. 1975) (stating in dicta that the FBI has some duty to ensure that NCIC information is accurate). *Accord* Testa v. Winquist, 451 F. Supp. 388, 395 (D. R.I. 1978). Although it is the responsibility of the individual NCIC agencies to ensure the accuracy of the records they enter into the system, the FBI should bear the ultimate burden of ensuring that the NCIC is a sufficiently reliable source for purposes of the fourth amendment. The large number of NCIC agencies necessitates that a single entity maintain discipline within the system.

procedures.[71] These include: quality control checks;[72] automatic removal of records after they are on file for a prescribed period of time;[73] and the periodic furnishing of lists of all records on file for validation by the agencies that entered them.[74] Compliance with these procedures also should be examined by the courts in determining whether the conduct of the sending agency is reasonable.

IV. Conclusion

Where a criminal charge stems from a search incident to an arrest based on inaccurate computer information and the defendant moves to suppress the evidence seized on the ground that the fourth amendment standard of probable cause was not met, the court must address two issues: first, whether the arresting officer acted reasonably pursuant to the information; and second, whether the agency that disseminated the information acted unreasonably in allowing the information to become inaccurate. If either the arresting officer or the sending agency acted unreasonably, the arrest should be struck down as not having satisfied the probable cause requirement of the fourth amendment. Where both have acted reasonably, however, the arrest should be upheld despite any inaccuracy. The fourth amendment requires adherence to standards of reasonableness and reliability, not certainty. The deterrent value of the exclusionary rule is not advanced where an arrest is invalidated in the absence of unreasonable police conduct.

---

71. NCIC Operating Manual § 1.3, at Intro-3 (May 1, 1981).

72. The FBI NCIC personnel periodically check records entered into the system for accuracy. *Id.* § 4.2.1, at Intro-62 (Nov. 1, 1980). If a check reveals an apparently erroneous record, the NCIC will advise the control terminal agency and the originating agency (the agency that entered the record into the system) of the record and request that it be verified, changed, or cancelled within 24 hours. If neither a response is received nor corrective action is taken during that time period, the NCIC is supposed to cancel the record. *Id.* § 4.2.3, at Intro-64 (Nov. 1, 1981).

73. The FBI periodically "purges" the computer files. Unrecovered stolen vehicle records generally remain on file for four years before they are removed. Records concerning unrecovered vehicles wanted in conjunction with a felony remain on file for 90 days after entry; if a longer period is desired, the vehicle must be re-entered. Records concerning wanted persons remain on file indefinitely until action is taken by the originating agency to clear the record. 46 Fed. Reg. 22499 (1981).

74. The NCIC periodically prepares listings of records on file, and mails them to the appropriate control terminals who in turn disseminate the records to the originating agency. The Vehicle and Wanted Person files are sent out for validation twice yearly. NCIC Operating Manual § 4.3.1, at Intro-65 (Nov. 1, 1981). The control terminal must certify to the NCIC that all records under its service jurisdiction are accurate. If a control terminal agency fails to certify any validation listing to the NCIC within 75 days, the NCIC is supposed to purge all of that state's unvalidated records. *Id.* § 4.3.2, at Intro-66 (Nov. 1, 1980).

To aid in the determination of whether the police agencies involved in an arrest based on inaccurate NCIC information satisfied probable cause, the courts should take judicial notice of NCIC policies and procedures. At a minimum, the courts should mandate that present NCIC safeguards be followed by NCIC user agencies.

Patrick Hand