



1976

Computerized Criminal Justice Information Systems: A Recognition of Competing Interests - An Introduction

Lawrence J. Beaser

Follow this and additional works at: <https://digitalcommons.law.villanova.edu/vlr>



Part of the [Criminal Law Commons](#), and the [Criminal Procedure Commons](#)

Recommended Citation

Lawrence J. Beaser, *Computerized Criminal Justice Information Systems: A Recognition of Competing Interests - An Introduction*, 22 Vill. L. Rev. 1172 (1976).

Available at: <https://digitalcommons.law.villanova.edu/vlr/vol22/iss6/4>

This Symposia is brought to you for free and open access by Villanova University Charles Widger School of Law Digital Repository. It has been accepted for inclusion in Villanova Law Review by an authorized editor of Villanova University Charles Widger School of Law Digital Repository.

COMPUTERIZED CRIMINAL JUSTICE INFORMATION
SYSTEMS: A RECOGNITION OF
COMPETING INTERESTS

AN INTRODUCTION

LAWRENCE J. BEASER†

The purpose of this symposium is to discuss whether certain types of information should be computerized in a large, automated criminal justice information system which is intended to provide data to a number of criminal justice agencies. To the extent that specific categories of data are discussed, the participants have been asked to focus on the computerization of three such categories: information of arrests both that do and do not result in conviction; personal history information; and medical history information. Also to be discussed are the competing interests which are affected by any such computerization.

This symposium concerns only information gathered by criminal justice agencies. By this is meant either a court or other government agency which as its principal function, "performs the administration of criminal justice."¹ Thus the term includes not only the police and the courts, but also prison systems, probation and parole systems, district attorneys, and so on.²

† Counsel to the Governor, Commonwealth of Pennsylvania; Member, Governor's Task Force on Criminal Justice Information Systems. B.A., University of Pennsylvania, 1967; J.D., Harvard University, 1970.

1. The Law Enforcement Assistance Administration [hereinafter cited as LEAA] Regulations, 28 C.F.R. § 20.1-38 (1976), define the term "criminal justice agency" to mean "(1) courts; (2) a government agency or any subunit thereof which performs the administration of criminal justice pursuant to a statute or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice." 28 C.F.R. § 20.3(c) (1976). Also, "administration of criminal justice" is defined to mean

performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history record information.

Id. § 20.3(d) (1976).

2. Compare the definition of "criminal justice agency" contained in the LEAA Regulations, *supra* note 1, with the definition of "criminal justice agency" contained in the *Dictionary of Criminal Justice Data Terminology*, U.S. Dept. of Justice, Law Enforcement Assistance Administration, Nat'l Criminal Justice Information and Statistics Service, First Edition 1976, which was prepared for LEAA by SEARCH Group, Inc., Sacramento, Cal.:

Any court with criminal jurisdiction and any other government agency or subunit, which defends indigents, or of which the principal functions or activities consist of the prevention, detection and investigation of crime; the apprehension, detention and prosecution of alleged offenders; the confinement or official

Moreover, only computerized information systems designed to link together a number of criminal justice agencies are being discussed. In the interest of time and simplicity, this symposium is not directly addressing specific problems created by record keeping within one criminal justice agency, except to the extent that the issues are the same as must be faced with regard to a larger, multiagency computerized criminal justice information system.

Finally, manually maintained records are not being discussed. The focus of this symposium is only on automated criminal justice information systems.³

In Pennsylvania, a discussion limited to automated systems eliminates from consideration criminal justice information systems maintained at present by the state government. The Governor's Task Force on Criminal Justice Information Systems⁴ has decided that the Commonwealth will not computerize the Pennsylvania State Police's criminal history records. In November of 1976, Lieutenant Governor Kline testified before the Pennsylvania House Appropriations and Judiciary Committees that Pennsylvania did not maintain a centralized computer history file nor did it contemplate resort to one in the future.⁵

Such a computerized criminal justice information system does exist in Philadelphia. The original scope of the Philadelphia Justice Information System (PJIS) was to collect and disseminate, by computer, all the information that the various Philadelphia criminal justice agencies would need to accomplish their functions.⁶ However, the guidelines promulgated for PJIS strictly limit the types of information which may be placed in the PJIS computer.⁷

correctional supervision of accused or convicted persons, or the administrative or technical support of the above functions.

Id. The agency for whom information is being collected and to whom information will be disseminated is a factor to be taken into account in determining whether the "computerization burden," discussed in the text accompanying notes 27-31, *infra* has been met.

3. The automated criminal justice information system being discussed here is not necessarily equivalent to a "criminal history record information system," which is the subject of the LEAA Regulations. See 28 C.F.R. § 20.3(a) (1976). One of the questions for discussion at this symposium is whether computerized data should be limited to some or all "criminal history record information" as defined in 28 C.F.R. § 20.3(b) (1976).

4. The Governor's Task Force on Criminal Justice Information Systems was established by Pennsylvania Executive Order No. 1975-10, 4 Pa. Code § 5.41-.47 (1975).

5. *Hearings on the Pennsylvania Plan for Privacy and Security of Criminal History Record Information Before the Commonwealth of Pennsylvania House of Representatives Appropriations and Judiciary Comm.*, at 10-11, November 4-5, 1976.

6. *Id.* at 288.

7. *Id.* at 224.

Despite the position adopted by Pennsylvania state government, the question of whether to computerize information in a criminal justice information system will continue to be debated throughout Pennsylvania and the rest of the nation. There is always concern that policies of one Governor may be changed by his or her successor and computer system guidelines may be amended in the future. Also, as automated data processing technology becomes more sophisticated, and perhaps less expensive, additional governmental bodies will confront the question of whether to computerize criminal justice information. In addressing this question, a number of difficult policy issues must be faced.

One such issue is, in the words of Professor George B. Trubow of the John Marshall Law School, the problem of "aggregated data."⁸ As Professor Trubow has stated:

The question is, does the mere fact of collecting information and marshalling it into a profile or "dossiere" change the nature of the information itself? It has been argued that since the ordinary criminal record is merely a compendium of separate public records established over a period of time, the mere fact of compilation makes no difference, and the compilation should be as accessible as were any of the entries at their respective point in time. That argument begs the question. Policy analysis is needed to clarify what, if any, impact arises from the action of government or anyone else in gathering into one place a series of possibly related but disjointed public happenings or events.⁹

The capabilities of today's computers, not only to aggregate vast amounts of data but also to sort and cross-correlate this material, can change the fundamental nature of much of that information. With computer technology, society has acquired the unprecedented ability to take information which once was in an unusable or barely usable form and make it instantly accessible.¹⁰ Access to unusable or barely usable information is fundamentally different from access to easily accessible and usable data.

As in many other areas of our lives, the advent of advanced computer technology has made a major change in the potential of

8. Trubow, *Informational Privacy and the Policy Foundations for Criminal Justice Information Management*, Advisory Bulletin No. 3, SEARCH Group, Inc., Sacramento, Cal., 35-38 (1976).

9. *Id.* at 38.

10. Cf. Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 MICH. L. REV. 1089 (1969): "With considerable justification, modern information-transfer networks have been described as a global electronic equivalent of the biological central nervous system because of their unprecedented ability to create awareness and responsiveness to human problems, and to provide a massive store of information subject to instant recall." *Id.* at 1245.

criminal justice information systems. In the past, these systems' capacity to collect, store and disseminate information was limited. Their inefficiency has always been one of the chief protections of individual privacy.¹¹

Former United States Senator Sam Ervin has referred to this as the "benign inefficiency of . . . file-drawer record systems".¹² Senator Ervin has observed:

Until very recently, significant amounts of information were not collected about individuals and therefore were not available to others. Use of information collected and kept on a decentralized basis is slow, inefficient and frustrating. It requires an immense effort to collect information on a specific individual from a variety of different agencies, and then to have it sent out to the agency requesting it. . . .

This decentralization, of course, is being radically changed by computerization and remote access through data networks.¹³

Also, computers are able to provide information in different forms than were previously available.¹⁴ A computer-prepared dossier, pulling together information culled from thousands or millions of documents or transactions is much more than the sum of its data bits.

The computer's capacity to aggregate data, whether one looks at it as an ability to create new information or to transform heretofore unusable facts into useful information, must be carefully considered when deciding what to computerize or even, when something is computerized, whether certain persons should have access to it. It is

11. See *Hearings on Criminal Justice Data Banks Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 93d Cong., 2d Sess. 147 (1974) (Sup. Doc. No. Y4. J89/2: C86/13/974 v.1) [hereinafter cited as *1974 Hearings*]. The then Attorney General William B. Saxbe testified:

In the past a criminal justice agency's capacity to collect, store and disseminate data was limited. Most systems were manual in nature and the very inefficiency of these systems was one of the chief protections of individual privacy, even recognizing that these manual systems were difficult to update and contained inaccurate information which was sometimes used to the detriment of the individual.

The scattering of data and files and the inefficient means for accessing data all served to reduce the scope and effectiveness of pre-computer information systems. The widespread use of computers and sophisticated interstate transmission networks, including potential satellite transmission for connecting these computers, has removed much of the protection the inefficiency of previous systems may have provided to personal privacy.

Id.

12. *Id.* at 18.

13. *Id.* See Miller, *supra* note 10, at 1109.

14. Cf. *Security and Privacy Considerations in Criminal History Information Systems*, Technical Report No. 2, SEARCH Group, Inc., Sacramento, Cal. (1970) which stated that "a computerized file can be quickly searched by whatever data elements it contains, such that compilations of subjects can be prepared with respect to certain characteristics contained in the file." *Id.* at 6.

too simplistic to state: "X" had access to the underlying, not particularly useful data, therefore "X" should have automatic access to the highly useful computerized information.

This ability of automated equipment to aggregate data, can lead to potential abuses and invasions of privacy. One example of this potential for abuse occurred early in 1973. At that time Pennsylvania state officials learned that the federal government was instituting a data collection system called CODAP — "Client Oriented Data Acquisition Process."¹⁵ Under CODAP, all drug programs in the United States would have been forced to supply for the federal government's computers — including criminal justice computers — enough information to construct something called a "unique identifier" of each patient.

As the name implies, this "unique identifier" is a means by which data from an individual may be identified as coming from that person. The name of the person would not be used, but the various data elements, we were told by our computer experts, could identify a person as indelibly as a fingerprint.

In addition, another program was simultaneously being put into effect. This was called DAWN — "Drug Abuse Warning Network." Using the same "unique identifier" as CODAP, this program would have resulted in surveillance from birth to death of persons with drug problems. DAWN was to be put into place in all hospital emergency rooms, for all hospital inpatients, at crisis intervention centers, and even at all medical examiners' and coroners' offices. Any patient who showed any signs of drug abuse, or admitted to drug abuse, would find himself or herself with a lifetime federal drug abuse record.

Members of Governor Shapp's administration became increasingly alarmed, especially when it was discovered that the federal government was planning to establish a national registry to trace drug abusers anywhere in the United States.

As a result of action by Pennsylvania, together with Massachusetts, the two systems were changed so that all information which could identify an individual was deleted.

15. The testimony of David Selig, the then Director of the Dangerous Drugs Advisory Commission for the state of Illinois before the Senate Judiciary Committee in 1974 characterizes the program's potential impact on confidentiality as the encroaching Federal policy of tying Federal funding to the release of confidential information by the states to the Federal agency It is happening more and more. Specifically, in my area, where the Department of Health, Education, and Welfare [is] requiring information on CODAP. Now they have another title, that if you want Federal money to fight drug abuse you are going to have to give confidential information. It is causing problems and it is burgeoning into other areas.

1974 *Hearings*, *supra* note 11, at 290.

If the system, as originally conceived, had become effective, individuals who innocently had gone to treatment centers with a medical problem¹⁶ would have been branded for life as drug abusers. Otherwise inaccessible information would have been made easily available by use of advanced technology. The computer's potential to aggregate otherwise not readily accessible data could have resulted in abuses affecting many citizens.¹⁷

Computerization of information by criminal justice agencies is not a problem which can be ignored. In many areas decisionmakers in the criminal justice system must answer the practical question of whether or not to utilize the tremendous speed and memory of today's computer technology¹⁸ to store and to retrieve information.

The policy considerations are not one sided. As is ordinarily the case when our society faces legitimate, antagonistic policy questions, there must be a balance of these interests.¹⁹ As former United States Attorney General Elliot Richardson has noted:

Philosophically, the problem can be stated quite simply. On the one hand, we must be concerned about social order; on the other we must be concerned about individual liberty and/or autonomy. However, the balance between these two guiding principles is always hard to strike in our society because of our ethical and Constitutional commitment to their interdependence.²⁰

There are three main interests which must be balanced in discussing whether to computerize information of the types discussed here today. The first interest is each individual's right of

16. The Pennsylvania Drug and Alcohol Abuse Control Act, P.L. 221, No. 1972-63 (codified at PA. STAT. ANN. tit. 71 § 1690.101-.115 (Supp. 1977-78)). The act declares that "[d]rug and alcohol abuse or dependence shall be regarded as a health problem, sickness, physical and mental illness, disease, disability, or similar term, for purposes of all legislation relating to health, welfare, and rehabilitation programs, services, funds and other benefits." *Id.* § 1690.110.

17. *Cf.* 1974 Hearings, *supra* note 11, at 290.

18. Senator Barry Goldwater has testified that

Revolutionary changes in data storage have taken place or are imminent. Computer storage devices now exist which make it entirely practicable to record thousands of millions of characters of information, and to have the whole of this always available for instant retrieval.

For example, the National Academy of Sciences reported in 1972: "That it is technologically possible today, especially with recent advances in mass storage memories, to build a computerized on-line file containing the compacted equivalent of 20 pages of typed information about the personal history and selected activities of every man, woman, and child in the United States, arranging the system so that any single record could be retrieved in about 30 seconds."

1974 Hearings, *supra* note 11, at 140 (footnote omitted).

19. 1974 Hearings, *supra* note 11, at 174. *But cf.* Emerson, *Legal Foundations of the Right to Know*, 1976 WASH. U. L. Q. 1, 21.

20. 1974 Hearings, *supra* note 11, at 174.

privacy.²¹ A second interest is the public's right to know what its government is doing.²² The third interest is the generalized interest of the people in having an effective and efficient government.²³

As in most areas involving individual rights, especially the right of privacy, there is substantial tension between the competing policy issues. Former United States Deputy Attorney General Harold R. Tyler, Jr., has observed this conflict in a slightly more limited context as follows:

All legislation designed to protect individual rights of privacy involves a tension between the public's right to know and the individual's right to preserve a certain zone of privacy into which the public cannot intrude. . . . If records of arrest, court proceedings, and correctional decisions are not publicly available, then the public is not only generally uninformed about its criminal justice process, but individuals risk all of the

21. In his famous dissent in *Olmstead v. United States*, 277 U.S. 438, 478 (1928) Justice Brandeis referred to the "right to be let alone" as "the most comprehensive of rights and the right most valued by civilized men." Though the right to privacy has been described as being "a notion of formidable obscurity," 1974 *Hearings, supra* note 11, at 439, it certainly has grown into an important, constitutionally based liberty. As was noted in *Roe v. Wade*, 410 U.S. 113 (1973),

The Constitution does not explicitly mention any right of privacy. In a line of decisions, however, going back perhaps as far as 1891, the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution. In varying contexts, the Court or individual Justices have, indeed, found at least the roots of that right in the First Amendment; in the Fourth and Fifth Amendments; in the penumbras of the Bill of Rights; in the Ninth Amendment; or in the concept of liberty guaranteed by the first section of the Fourteenth Amendment. These decisions make it clear that only personal rights that can be deemed "fundamental" or "implicit in the concept of ordered liberty" are included in this guarantee of personal privacy.

Id. 152-53 (citations omitted). See, e.g., Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); Comment, *A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision*, 64 CALIF. L. REV. 1147 (1976); The Nat'l Ass'n of Attorneys Gen. Committee on the Office of the Attorney Gen., *Privacy: Personal Data and the Law*, Raleigh, N. C. (Nov., 1976).

22. This right was acknowledged from the outset: "A popular government, without popular information or the means of acquiring it, is but a prologue to a farce or a tragedy; or perhaps both. Knowledge will forever govern ignorance. And a people who mean to be their own governors, must arm themselves with the power knowledge gives." Letter from James Madison to W. T. Barry, August 4, 1822, in 9 WRITINGS OF JAMES MADISON 103 (G. Hurst ed. 1910). See Emerson, *supra* note 19; Nat'l Ass'n of Attorneys Gen., *supra* note 21 at 8.

23. It has been noted that

[t]here are other interests, however, which must be considered in determining the weight of a particular claim of privacy. All individuals in the society share an interest in an effective government. The government's need to obtain information about individuals in order to formulate and implement its policies may outweigh the individual's interest in disclosural privacy.

Nat'l Ass'n of Attorneys Gen., *supra* note 21, at 7.

Economic factors may also be a consideration because there is also an interest in having an efficient government. But the decision to computerize should not be made merely because it is economically feasible or even less expensive to utilize computer technology. See text accompanying notes 27-31 *infra*.

dangers inherent in secret arrests, Star Chamber proceedings, and banishment to secret prisons. Yet if a past error, already paid for, can follow an individual for the rest of his life, threatening his employment opportunities and his acceptance in the community, our hopes of rehabilitating offenders through improved correctional services are impeded.²⁴

As Pound put it, this situation is "one of compromise; of balancing conflicting interests and securing as much as may be with the least sacrifice of other interests."²⁵

In weighing the competing interests, there are very real dangers inherent in criminal justice agencies' computerizing of sensitive information, such as medical records, a person's association with other persons or groups and so on. "While advances in technology contribute to more effective and efficient law enforcement, they also greatly increase the opportunity for abuses."²⁶

In the decisionmaking process concerning whether to place information in a computerized criminal justice information system, those who propose such computerization should bear a clear burden of showing that such computerization is necessary and that the balance of interests should be tipped in favor of computerized recordkeeping.²⁷

This computerization burden should extend individually to each data element. Every item of information collected about people and fed into a criminal justice system computer should require justification.²⁸ We cannot permit the collection of data in automated criminal

24. *Hearings on H.R. 8227 Before the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary*, 94th Cong., 1st Sess. 77 (1975) (Sup. Doc. No. Y4.J89/1: 94-68) (Statement of Deputy Attorney Gen. Harold R. Tyler).

25. R. Pound, *CRIMINAL JUSTICE IN THE AMERICAN CITY* 18 (1922), cited in 14 *HARV. J. LEGIS.* at 24 (1976).

With regard to the "clash between the right of privacy and the right to know" Professor Thomas I. Emerson suggests that "ad hoc balancing" is the "least useful path to follow." Emerson, *supra* note 19, at 21. While admitting that "some element of balancing would probably be found in any test," Professor Emerson would solve any such conflict by giving precedence to the right of privacy. *Id.* at 22. With regard to computerized criminal justice information systems, the proposed "computerization burden," while not giving complete precedence to the right of privacy does weigh the scales in privacy's favor. See text accompanying notes 27-31, *infra*.

26. Cooper and Zehner, *Privacy: The Evolution of an Issue*, Advisory Bulletin No. 3, SEARCH Group, Inc. 1, 19 (1976).

27. Whether certain information should be collected at all is another issue altogether. The question here is only whether information of a sensitive nature should be computerized.

28. Cf. Miller, *supra* note 10, at 1214 wherein the author stated:

[I]f informational privacy is to be protected, it is crucial to screen data initially to prevent some of it from being placed in the system.

Extremely sensitive personal information — for example, records of mental illness, or inherently "soft" data, such as psychological test results — normally should be excluded from large multiaccess systems even if the files customarily

justice information systems just because excess computer capacity exists.

The interlocking of computer banks should require similar, if not stronger, justification. Information stored in one computer becomes even more usable, and subject to abuse, when it can be correlated with data contained in other computer systems. Then too, the interlocking of computer banks can increase the very real potential for dissemination of inaccurate information. Indeed, the ease of disseminating inaccurate data is one of the great potential hazards to be faced when information is fed into a computer.

The concept of a "computerization burden" should not be construed as being antitechnology or against the use of technology.²⁹ The societal interest in an efficient and effective criminal justice system is strong and technological developments in appropriate cases can assist in improving the system. But this interest must always be weighed against the very real dangers to individual privacy from the use of this same technology.³⁰

The "computerization burden" approach can be used by decision makers in resolving conflicts between the competing interests. This is the type of analysis which the Governor's Task Force on Criminal Justice Information Systems used in making the decision not to computerize the Pennsylvania State Police's criminal history record files.³¹

In discussing what data is to be computerized in a large, multiagency criminal justice information system, a balance must be reached between the competing interests, with the proponents of computerization clearly bearing the computerization burden.

The debate concerning the right of privacy, the public's right to know, and the needs of government for greater efficiency, will continue and is healthy for our society. The ability to collect, collate and disseminate data has so increased as to make the world of 1984, as envisioned by George Orwell, a present day possibility.

are stored in a secure area removed from the central processor. Unless there is some definable and compelling reason to include this type of information in a multiaccess system, every effort should be taken to keep it out of the information flow.

Id. (citation omitted).

29. In his book, *DOSSIER* (1974), Areyh Neier observed that "[c]omputerization makes consolidation of information far easier than is possible if each of the record-maintaining agencies does its work manually." *Id.* at 162. However, he states that computers are not "the villain" since "the two largest and most harmful data banks" he examines are both "old-fashioned manually operated systems." *Id.*

30. See Miller, *supra* note 10, at 1173-74.

31. See text accompanying notes 4 & 5 *supra*.