Privacy, Law Enforcement, and Public Interest: Computerized Criminal Records

Joan Uda
Systematic recordation and dissemination of information about individuals is a form of surveillance and control which may easily inhibit freedom to speak, to work, and to move about in this land. If information available to Government is misused to publicize past incidents in the lives of its citizens the pressures for conformity will be irresistible. Initiative and individuality can be suffocated and a resulting dullness of mind and conduct will become the norm. ... The present controversy ... must be viewed in this broadest context. In short, the overwhelming power of the ... Government must be held in proper check.¹

INTRODUCTION

We in Montana, like the rest of our world, have entered an era of disturbing and unprecedented capacity for data gathering, storage, processing, and dissemination. We owe this abundance to computer technology, the implications of which have not been lost upon government or private enterprise. According to Senator Sam Ervin, Chairman of the Senate Subcommittee on Constitutional Rights, and Senate leader in the fight for “data privacy,” the federal government alone has over 900 computer banks,² containing information about tens of millions of private citizens. Commercial enterprise is keeping pace: for example, the Atlanta-based Retail Credit Company, which is in the business of supplying credit information, has files on more than forty-five million people, obtained by a staff of seven thousand investigators.³

Montana is currently faced with an extremely important computer question: whether or not to establish a computerized criminal data system, which will eventually be interfaced with other similar state and federal systems. At present Montana has no such system; criminal record data is kept by the Montana Department of Justice’s Identification

²In 120 CONG. REC. S 1295-96 (daily ed. Feb. 5, 1974), Senator Sam Ervin gave a figure of ‘‘over 800’’. On a subsequent N.B.C. news special in the spring of 1974, he said there were 910 federal computerized data banks.
³A. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 69 (1971) [hereinafter cited as MILLER]. Miller notes that these investigators interview ‘‘employers, former employers, references, fellow club members, neighbors and former neighbors [and] financial professional people,’’ and that much of the information they elicit is unverified and little better than gossip.
⁴REVISED CODES OF MONTANA, § 82A-1202(1) (1947) [hereinafter cited as R.C.M. 1947], abolished Montana’s earlier State Bureau of Criminal Identification and Investigation and transferred its functions to the Department of Justice. These functions are set out in R.C.M. 1947, §§ 80-2002 to 80-2006, including (1) maintaining records of identification information such as fingerprints, photographs, and descriptions, on ‘‘all persons . . . convicted of a felony within the state, and of other well-known and habitual criminals,’’ § 80-2002; (2) notifying local law enforcement agencies if a particular subject on whom it receives information is a
Bureau, which, though tied into a teletype network, operates only manual files.

Much of the impetus to form an extensive interstate criminal data system comes from the federal government, through the Law Enforcement Assistance Administration (L.E.A.A.), which was established within the United States Department of Justice to administer funds made available by the Omnibus Crime Control and Safe Streets Act of 1968. The Montana Board of Crime Control, which administers L.E.A.A. funds within Montana, has appointed a Security and Privacy Task Force to study the security and privacy issues raised by such systems and to draft Montana legislation on the subject.

Montana is thus presented with a set of difficult decisions involving both policy and implementation. These decisions, because of their ultimate social impact, must receive our most thoughtful attention. This comment will explore some of the decisions to be made, with an eye to the competing interests of privacy and law enforcement, and will suggest some possible solutions.

**PRIVACY AND COMPUTERS: THE LARGER CONTEXT**

Privacy is, in the words of Mr. Justice Brandeis, "the right to be let alone." In his famous dissent to *Olmstead v. United States*, he said:

> The makers of our Constitution . . . recognized the significance of man's spiritual nature, of his feelings and of his intellect. . . . They sought to protect Americans in their beliefs, their thoughts, their.

According to David Clouse, Acting Bureau Chief, Montana badly needs mandatory reporting provisions, including dispositions, with strict penalties for violations. Apparently fewer than 20 percent of the Bureau's arrest records contain dispositions, because information is entered into the Bureau's files only upon receipt of fingerprint cards. Unless the subject pleads guilty or entry is delayed until after disposition, the original entry will not contain the disposition; and the local law enforcement agencies rarely follow up with another fingerprint card to enter the disposition. The Bureau has no power to require this followup. Telephone Conversation with David Clouse, Oct. 11, 1974.


The Crime Board has been designated by the governor as the "state planning agency" under the Omnibus Crime Control and Safe Streets Act of 1968 and must "perform the functions assigned to it under the act." R.C.M. 1947, § 82A-1207(4). Relevant federal provisions may be found at 42 U.S.C. §§ 3721 to 3738 (1970), Law Enforcement Assistance Administration, Subchapters II and III.

emotions and their sensations. They conferred as against the govern-
ment, the right to be let alone—the most comprehensive of rights and
the right most valued by civilized men.8

Mr. Justice Douglas has expressed the relationship between privacy
and individual freedom most succinctly: "The right to be let alone is
indeed the beginning of all freedom."19

There is increasing concern about the proliferation of data and its
impact upon privacy and personal liberty. The cybernetic revolution
poses particular threats because huge masses of data create the pos-
sibility of large-scale social control and also promote individual docility.

As every man goes through life he fills in a number of forms for
the record, each containing a number of questions. . . . There are
thus hundreds of little threads radiating from every man, millions
of threads in all. . . . They are not visible, they are not material,
but every man is constantly aware of their existence [and] natural-
ly develops a respect for the people who manipulate the threads.11

Professor Arthur R. Miller of Harvard Law School, one of the
country's foremost experts on computers and privacy, characterizes the
pulling together of these threads as a "record prison"—a "womb to tomb
dossier" on every American, which can be made available nationwide to
undetermined and virtually uncontrolled data users.12 In 1971 Miller
estimated that there were more than 60,000 computers in the United
States,13 noting that "laser technology already makes it feasible to store
a twenty-page dossier on every American on a piece of tape that is less
than five thousand feet long."14

This computer capacity led Miller to the concept of "record prisons"
because the computer never forgets and never forgives. There is, in Christ-
tian terms, no possibility of redemption. In a computer record society,
a person has no latitude for youthful or careless mistakes,15 no room for
personal eccentricity,16 and will ultimately learn to keep his mouth shut
and his protests to himself,17 lest the computer learn and tell.

8Id. at 478-79.
9Public Utilities Comm'n v. Pollak, 343 U.S. 451, 467 (1952) (Douglas, J., dissent-
ing).
10A. SOLZYHENITSYN, CANCER WARD, as read into the Congressional Record by Senator
Sam Ervin, supra note 2 at § 1295.
11MILLER, supra note 3 at 39.
12Id. at 10.
13Id. at 12.
14See generally MILLER, supra note 3 at 105-122 (section entitled "The Little Red
Schoolhouse Goes Electric"), and Gough, The Expungement of Adjudication Records
of Juvenile and Adult Offenders: A Problem of Status, 1966 WASH. U. L. Q. 147,
168-78 (1966).
15Miller notes that congressional hearings on credit companies uncovered many files
containing remarks from anonymous sources such as "peculiar," "scatter-brained,"
"neurotic," and "psychotic," with no apparent medical or psychiatric foundation.
"Other files included remarks about the subject's drinking, aggressiveness, ethics,
associations, health, hobbies, and activities." Miller suggests that it is very likely
that personal antagonisms and prejudices greatly influence the contents of these
files. MILLER, supra note 3 at 70.
16See United States v. McLeod, 385 F.2d 734 (5th Cir. 1967) (civil rights workers
arrested and convicted in effort to disrupt a voter registration drive); Hughes v.
Every person has a need for privacy—for personal space in which to relax, to explore, to grow. All of us seek moments in which we “let down our hair,” are “off the record”—moments when we wish to be free from the prying of those who seek to evaluate who and what we are. Computerization means that we may be constantly evaluated by persons who never meet us, strangers to whom we are nothing more than isolated facts on a computer print-out. Those facts may be inaccurate, incomplete, stale—and we most often are unaware that the record exists. Thus, we may become locked in Miller’s “record prison,” where a collection of facts, perhaps accurate, perhaps not, becomes the sum of our lives.

Sensitivity to this problem leads to a definition of privacy as the right to control the flow of information about one’s self. According to Miller:

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.

Government has, of course, been keeping manual records for years, and these are also susceptible to abuse. But computerization presents problems of enormously greater magnitude. First, computerization allows collection of great quantities of personal data that was too expensive and time-consuming to collect under a manual system. What was not collected could not be disseminated. Second, manual systems were kept mostly on a decentralized basis and were widely scattered. Computer capacity allows virtually instantaneous centralization and dissemination. Third, information in manual systems has typically been quite superficial and often so out of date as to be virtually useless. Computers allow instant updating and cross-referencing from many sources of data. Fourth, it has been difficult to obtain access to much available information, since this often involved a search of bulky files and voluminous, isolated records. A computer system puts such data at one’s fingertips in a matter of seconds from a remote access terminal. Fifth, Americans have become increasingly mobile, making them difficult to keep track of. Computer systems using universal identifiers make it possible to track everyone from the cradle to the grave. Finally, in manual systems, insufficient data have been available to allow most people to interpret and infer revealing information about the data subjects. Computers make

---

Rizzo, 282 F.Supp. 881 (E.D.Pa. 1968) (police harassment of “hippies” to keep them from congregating in a public park, by making mass arrests with no intention of filing charges against them); United States v. Kalish, 271 F.Supp. 968 (D.P.R. 1967) (individual refused to step forward for induction on advice of counsel under agreement with the U.S. Attorney that no action would be taken; individual was immediately arrested, though he explained that other judicial proceedings were pending).

See generally A. Westin, Privacy and Freedom 8-22 (1967).

Miller, supra note 3 at 25.
interpretation much easier by amassing great amount of personally identifiable data.\textsuperscript{20}

The Identification Division of the Federal Bureau of Investigation has files containing "rap sheets"\textsuperscript{21} or fingerprint cards on more than twenty million persons.\textsuperscript{22} The Defense Department keeps industrial security files, including sensitive personal information, on more than a million and a half individuals.\textsuperscript{23} Huge amounts of sensitive personal data are contained in income tax, census, and social security files.\textsuperscript{24} This information is not invariably confidential.\textsuperscript{25}

In the mid-1960's Congress and privacy-minded citizens rebelled against the creation of a National Data Center, which was intended to centralize the statistical information gathering and processing of many federal agencies and departments.\textsuperscript{26} Opponents feared that the persons who would be responsible for its creation and administration were largely insensitive to its impact on privacy and freedom. It was potentially, a huge dossier-system on virtually every American.\textsuperscript{27} More recently, the General Services Administration requested $200,000,000 to set up a computer network, "FEDNET," to be shared by numerous federal agencies. Last July Congress refused to allow GSA funds to be used for "FEDNET."\textsuperscript{28} In the meantime, a number of federal agencies, departments, and bureaus are using time-sharing computer systems,\textsuperscript{29} indicating that, for the data-hungry federal bureaucrat at least, where there's a will, there's a method.

\textsuperscript{20}Id. at 26.
\textsuperscript{21}A "rap sheet" is an individual's criminal record. Exact contents vary from agency to agency, but at minimum it contains arrests and charges and sometimes dispositions.
\textsuperscript{22}120 CONG. REC. S 1295 (daily ed. Feb. 5, 1974). The Division has data on approximately sixty million arrests involving about nineteen million people and has about two hundred million sets of fingerprints on file. Menard, supra note 1 at 721.
\textsuperscript{23}120 CONG. REC. S 1295 (daily ed. Feb. 5, 1974).
\textsuperscript{24}MILLER, supra note 3 at 82, 131, 145 (income tax); 126-141 (census); 60-61 (social security).
\textsuperscript{25}Miller notes that the Internal Revenue Service has sold "aggregate income statistics about taxpayers broken down by Zip Code Number." Id. at 82. He also documents extensive transfers of information among federal, state, and local government agencies, id. at 146-153 and among federal agencies, id. at 141-145. Miller also points out "the informational backscratching" that exists in a number of areas, including law enforcement and corporate security.
Every sizable company, particularly those engaged in work for the government, maintains dossiers on large numbers of people . . . The total must be staggering . . . Because of their similarity in background and common interests, an informal, but effective, information transfer network exists among industry security officers and all segments of the law-enforcement fraternity. Thus, a security man man with a grudge (or for a price) probably can blackball someone and limit his ability to gain employment. Ironically, in one case of this type . . . the individual excluded from the job market had been both a law-enforcement and a corporate-security man himself for many years.
Id. at 149.
\textsuperscript{26}Id. at 56-57.
\textsuperscript{27}Id. at 56-59.
\textsuperscript{28}H.R. 15544, as amended July 31, 1974, Title IV, Sec. 3.
\textsuperscript{29}MILLER, supra note 3 at 60.
PRIVACY AND COMPUTERIZED CRIMINAL DATA

Computerization of personally identifiable criminal data shares all the problems associated with computerization of any personal data. It also presents some unique problems because of its extreme sensitivity and the destructive personal consequences when such data is misused.

On the other hand, there is no question that computerization has been a great boon to law enforcement. For example, a Missoula, Montana, patrolman in a radio car can have an N.C.I.C. check run on a possible stolen vehicle in a matter of seconds. He can also very quickly determine if there is an out-of-state "want" on a particular individual. In a society annually appalled by a rise in serious crime rates, it is difficult to argue with any means which offers more effective crime prevention and detection.

One area of increasing controversy is the use of arrest records, particularly raw arrest records which contain no dispositions, and arrest records of persons who have been acquitted or against whom charges have been dismissed.

In the United States, an ancient precept of criminal law is that a person is innocent until proven guilty. As noted by the Washington State court of appeals:

"Few things have been as basic to our legal system as the presumption of innocence, until proof of guilt beyond a reasonable doubt. In fact, the very word acquittal is defined to mean "judicially discharged from an accusation, . . . charge, or suspicion of guilt." An arrest . . . proves nothing so far as the actual conduct of the person arrested. . . . [O]nly a conviction carries legal significance as to a person's involvement in criminal behavior."

-National Crime Information Center, of the Federal Bureau of Investigation [hereinafter referred to as N.C.I.C.]. N.C.I.C. contains information on stolen property and persons with outstanding arrest warrants. By 1971 about three thousand remote access terminals connected local law enforcement agencies with N.C.I.C. About one-third tie in directly to the FBI's computers, and the other two-thirds tie in to state computer systems that have access to N.C.I.C. Id at 147.

-Id.

-There is no doubt that computerization offers much help. See President's Commission on Law Enforcement and Administration of Justice, Task Force Report: Science and Technology 68-70 (1967).

-About thirty-five percent of the FBI's arrest records do not contain dispositions. Id. at 76. See discussion concerning Montana, supra note 4.


A mere arrest, or an arrest followed by complete exoneration, may, however, have a disastrous impact on an individual’s life and career.

Perhaps the most sensitive area is employment. One survey by the New York Civil Liberties Union showed that 75 percent of New York area employment agencies refuse to refer an applicant with an arrest record, regardless of disposition. Another survey, covering 75 employers, revealed that 66 of them would not consider an applicant who had been acquitted of an assault charge.

The possibilities for abuse of national criminal data are very nearly staggering. The FBI’s Identification Bureau has jurisdiction over arrest records; and by federal statute, the Attorney General or officials appointed by him must:

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

Rulings by the Attorney General interpreting the statutory authority provide that the Director of the FBI shall:

Conduct the acquisition, collection, exchange, classification, and preservation of identification records, including personal fingerprints voluntarily submitted, on a mutually beneficial basis, from law enforcement and other governmental agencies, insurance companies, railroad police, national banks, member banks of the Federal Reserve System, FDIC-Reserve-Insured Banks, and banking institutions insured by the Federal Savings and Loan Insurance Corporation; provide expert testimony in Federal or local courts as to fingerprint examinations; and provide identification assistance in disasters and in missing persons type cases including those from insurance companies.

The FBI certainly does not disseminate such information to all comers, but it is required by law to disseminate it to the agencies listed above as well as to federal agencies for record checks on all prospective federal employees. And, although the FBI may cancel the exchange of records with an agency which allows improper dissemination, it

---


7 Id.


9 28 C.F.R. § 0.85 (b) (1949-53 Comp.).

10 Exec. Order No. 10,450, 3 C.F.R. 936 (1949-53 Comp.), 5 U.S.C. § 7311 (1964). According to Menard v. Mitchell, supra note 1 at 722, the Civil Service Commission and the military submit the largest number of fingerprints to the Identification Bureau. The Bureau receives about 29,000 fingerprints a day, approximately 13,000 from law enforcement agencies concerning arrests and the remaining 16,000 from other sources.

The Division, broadly speaking, considers any state, city or county official to be authorized to receive information if the agency has something to do with law enforcement or if it is authorized by statute, ordinance, or rules to fingerprint applicants for employment or for a permit or license.

Id. at 721. The court in Menard included an appendix, "Sample of Persons required to be Fingerprinted by State or Local Statute, Ordinance or Rule":

Glendale, Arizona:
Taxicab drivers . . . traveling merchants . . . solicitors or canvassers . . .
has no practical means to supervise or control the information once it leaves the central file and has no sanctions beyond mere cancellation.\(^42\)

It is naive to think that FBI or other law enforcement information never reaches employers. A Massachusetts grand jury has recently been investigating evidence that state police officers were selling police records to private employers,\(^43\) and one study revealed that employers in St. Louis and Baltimore had regular access to police records.\(^44\) In New York, Washington, D.C., Los Angeles, San Francisco, Chicago, and Boston, such access apparently depended on the status of the employer; it was reserved for the influential.\(^45\)

Courts and legislatures are becoming more and more aware of the potential harm to an individual from the mere fact of having an arrest record. *State v. Pinkney*\(^46\) involved an 18-year-old defendant who was indicted for first degree murder. He was tried but the jury deadlocked; and while he was awaiting retrial several months later, other people confessed to the murder. He successfully petitioned to have all police records pertaining to this arrest, including those in the possession of any federal law enforcement agencies, expunged. The court said:

> It is the opinion of this Court that there exists in the individual a fundamental right of privacy, the right to be left alone. The potential economic and personal harm that result if his arrest becomes known to employers, credit agencies or even neighbors, may be catastrophic.\(^7\)

The court further quoted with approval from *Menard v. Mitchell*,\(^48\)

---

*Denver, Colorado:*
Any applicant for a driver’s license.

*District of Columbia:*
Auctioneers . . . junk dealers, mediums, parking lot attendants, pawnbrokers, second hand dealers . . . vendors . . . ABC licensees.

*Town of Manalapan, Florida:*
Every person employed in any club, any place handling liquor, beer or wine in any form, motels, hotels, apartment houses, health spas, hospitals, and all newspaper carriers over the age of sixteen years, service station employees . . . nurses . . . town employees . . . and all domestic servants in the town.

*Idaho:*
All real estate salesmen and brokers.

*Nevada:*
Every applicant for a license to practice medicine.

*North Carolina:*
Applicants for admission to the Bar.

*Provincetown, Massachusetts:*
All non-residents seeking employment.\(^7\)

*Id.* at 728. The *Menard* court noted, however, that ‘‘criminal record data is not sent directly to private employers,’’ except in a few defined instances. *Id.* at 722.


\(^{43}\) *Menard v. Mitchell*, supra note 1 at 722.


\(^{45}\) *Arrest Records—Protecting the Innocent*, supra note 34 at 632. The same writer records that, ‘‘[t]he least one major investigation agency has advertised police file checks as part of its services.’’ *Id.*

\(^{46}\) *Id.*


\(^{48}\) *Id.* at 924.

\(^{49}\) *Menard v. Mitchell*, supra note 36 at 490.

https://scholarship.law.umt.edu/mlr/vol36/iss1/4
a case in which the plaintiff, arrested for a crime which never occurred, sued for expunging of his arrest records. The United States Court of Appeals for the District of Columbia Circuit reversed the district court's granting of defendant's motion for summary judgment and remanded the case for trial. In remanding, the court said:

Information denominated a record of arrest, if it becomes known, may subject an individual to serious difficulties. Even if no direct economic loss is involved, the injury to an individual's reputation may be substantial. Economic losses themselves may be both direct and serious. Opportunities for schooling, employment, or professional licenses may be restricted or nonexistent as a consequence of the mere fact of an arrest, even if followed by acquittal or complete exoneration of the charges involved.

The court then explained other types of harm to the person with an arrest record, even one who is totally innocent:

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

Add to all of this the fact that at present few criminal justice agencies are governed by statutes or rules requiring a periodic purge of stale records, and it becomes appallingly clear that an arrest record, by the mere fact of its existence, may hound a person, even an innocent person, for the rest of his life.

**BALANCING THE PUBLIC'S INTERESTS:**
**PRIVACY AND LAW ENFORCEMENT**

It is obvious at this point that the public has two discrete, and to some extent conflicting, interests in the controversy over the proper handling and use of criminal records. On the one hand, we cannot ignore the valid needs of law enforcement; on the other, we must preserve

---

Menard v. Mitchell, [*supra* note 1].

Menard v. Mitchell, [*supra* note 36 at 490].

Id. at 490-491.


At least two bills introduced into the United States Senate on Feb. 5, 1974, would provide for purging or sealing of certain records at stated intervals. One is Senator Sam Ervin's "The Criminal Justice Information Control and Protection of Privacy Act of 1974" (S. 2963, Section 206); the other is "The Criminal Justice Information Systems Act of 1974" (S. 2964, Section 9), which was introduced by Senator Roman Hruska at the request of the Attorney General.
our hard-won personal liberties, not the least of which is "the right to be let alone." We might also question the meaning of "innocent until proven guilty beyond a reasonable doubt" in an era of wide dissemination of arrest records not followed by a plea or finding of guilty.

One of the most common justifications for the need to maintain all arrest records, regardless of disposition, is that of identification and apprehension of criminals.

As a means for identification and apprehension of criminals, an arrest record does serve the police community as a most valuable tool. Nation, state and citywide crime detection and prevention are based upon a system of information and communication. Statistical experience tells them that persons with arrest records commit a higher percentage of crimes than persons who do not have arrest records.53

The Washington State court of appeals has pointed out, however, that the usefulness of arrest records for purposes of crime prevention and detection rests upon two assumptions: one, that the arrestee actually committed the crime; and two, that his commission of that crime shows that he is likely to commit other crimes in the future.54 If the arrestee makes an affirmative showing of innocence, or if he is acquitted or charges against him are dismissed, the first assumption may be totally in error. The validity of the second assumption can be challenged if the first is faulty, and also, independently, in that certain types of criminal offenders tend to be repeaters and others do not. Thus, there are many situations where retention of arrest records is useless for purposes of detection and prevention of crime.

It has also been asserted that all arrest records must be kept indefinitely for administrative reasons. In Spock v. District of Columbia,55 the District of Columbia Court of Appeals said that all arrest records were necessary to prevent secret arrests, to be used in cases of alleged police misconduct, and to serve the legislature in its future deliberations.

The answer to the problem of secret arrests would seem to be that no one is suggesting that local arrest records not be made at all or that they be purged prior to disposition of the case or before a statutory interval for purging has run out.56 As to charges of police misconduct, surely local purging statutes can be drawn to take into account the date at which such claims would become stale. Finally, in regard to the legislature's need for arrest data to draw future legis-

53Eddy v. Moore, supra note 35 at 217.
55The real question in this comment is what should be allowed to go into the computer, not what type of record information should be retained in local law enforcement files. The latter is a separate and difficult question. States with purging or sealing statutes seem not to have found this an insurmountable problem, however. See authorities cited supra note 52.
lation, it is both possible and sensible to preserve statistical data without individual identifiers.

The problems of computerizing criminal data are, of course, much greater than those pertaining specifically to arrest records. On the side of law enforcement, instantaneous access to certain types of criminal data is extremely useful to officers in the field. Project SEARCH\(^5\) (SEARCH is an acronym for System for Electronic Analysis and Retrieval of Criminal Histories) points out:

[I]n most police "on scene" investigations where possible suspects are involved, the officer requires immediate knowledge of prior record to aid in making decisions regarding search, detention, or arrest.

Given factual knowledge of the occurrence of a crime and that the suspect was in the vicinity, the law enforcement officer's aim is to obtain sufficient information to determine the extent to which further police investigation should be conducted. For this purpose, it is necessary to quickly supply the investigator with sufficient data to pursue the case in an intelligent manner. Further information about the suspect is vital knowledge for the officer charged with arresting the subject; for example, does he have a record of violent behavior or of using lethal weapons?\(^6\)

SEARCH further notes that such information would help police determine: (1) the proper charge; (2) whether to issue a summons instead of making an arrest; (3) court jurisdiction; (4) whether the subject should be released on bail; (5) the subject's current criminal justice status (e.g., if he's already on bail, on probation or parole, and the like).\(^5\)

However, much of the data which SEARCH\(^6\) would gather into a computer system, under its proposed Model State Act for Criminal Offender Record Information, is extremely sensitive. It includes:

[R]ecords and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, rehabilitation and release.\(^6\)

This presents a whole range of privacy and security problems, not the least of which is the problem of using arrest records of exonerated persons in any of the ways mentioned above.\(^6\) Also, though such information may be useful, there are many situations where a person's past criminal record should not be used. For example, a person's past record should rarely be an important factor in determining probable

\(^5\)SEARCH started in June, 1969. Its purpose was to develop a prototype computerized criminal data system; and it was funded by L.E.A.A., see text supra note 6, and participating states. See, Project SEARCH Security and Privacy Publications, May 1973, Part I: Security and Privacy Considerations in Criminal History Information Systems, at 1, and Part III, Model Administrative Regulations for Criminal Offender Record Information, at 2 [hereinafter cited as Project SEARCH].

\(^6\)Project SEARCH, supra note 57, Part I at 2.

\(^7\)Id. One of the reasons SEARCH sees need for computerized inter- and intra-state criminal data systems is the mobility of the criminal population. Id. at 3.

\(^8\)Project SEARCH, supra note 57, Part II.

\(^9\)Id. at 15.

\(^1\)See text accompanying notes 58 and 59, supra.
cause. Yet it is quite possible that once such information is abundantly and easily available, it will be used improperly—even by generally well-intentioned and conscientious officers—simply because it is there.

In addition, system security is no less a problem in criminal data systems than in other systems containing sensitive information. Although it is beyond the scope of this paper to deal at length with system security, a few points should be made.

First, though it is possible to develop a system which is technologically very secure, this is extremely expensive—so expensive that perhaps only the military can afford it. Also, though the hardware and software may be secure, there is always the human factor. Careful screening of key persons allowed in the central processing area is both possible and desirable, but what of the thousands of remote access terminals across the country and the tens of thousands of persons who can and will operate them?

We should also keep in mind that we are not considering a manual system where an interested party, even if he should get improper access to sensitive files, would be limited as to the amount and quality of available data. A national network of interfacing criminal data computers offers, with a single and relatively brief access to only one terminal, huge quantities of high-quality information. Because of this, it may be worth the while of certain wealthy and powerful organizations to bend their efforts toward learning what the computer knows.

There is clearly a need to balance the competing public interests in effective law enforcement and individual privacy. The 1972 Montana Constitution provides a mandate in this regard, for it contains, in Article II, Section 10, an explicit, general right of privacy.

The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.

A past record, combined with many other factors, might help to establish "reasonable cause to suspect," as the term is used in R.C.M. 1947, § 95-719, Montana's Stop and Frisk statute, thus allowing brief detention for further investigation. Standing alone, however, a past record establishes nothing about present conduct.

The likelihood of this can be cited to lack of education or sensitivity to the destructive potential of such uses, the inability to overcome temptation, mutual backscratching, and the like. See discussion, supra note 43-45 and note 25.

Miller, supra note 3 at 242.

In 1971 there were from 7,000 to 8,000 agencies participating in information exchange with the FBI's Identification Division, of which about 3,750 were local law enforcement agencies. Menard v. Mitchell, supra note 1 at 721. Senator Ervin noted that when the N.C.I.C. computerized criminal data system is "fully operational," about 40,000 state and local police agencies will be tied into it. 120 Cong. Rec. S 1296 (daily ed. Feb. 5, 1974).

See discussion, supra note 20, comparing manual with computerized data systems.

This could include large corporations seeking information on employees, potential employees, and persons with whom they do business, not to mention large-scale criminal organizations, for which such data would be a veritable gold mine.
This provision is evidently unique among American constitutions, and its contours have yet to be interpreted and defined by the Montana supreme court. One thing seems certain, however; Section 10, by the use of the "compelling state interest" language, was intended to elevate the right of privacy in Montana to the status of a fundamental constitutional right.

Thus, the proper test for any state proposal involving collection and dissemination of personal data would seem to be whether the state can carry its burden of showing that the proposal is "necessary, and not merely rationally related, to the accomplishment of a permissible state policy." That is:

Where there is a significant encroachment upon personal liberty, the State may prevail only upon showing a subordinating interest which is compelling.

Several state courts have recently applied the compelling state interest test to arrest record cases. In *Eddy v. Moore*, Harriet Eddy sued for return of her photographs and fingerprints from the Seattle Police Department after assault charges against her were dismissed at trial. The court held that she was entitled to their return, noting:

We believe the right of an individual, absent a compelling showing of necessity by the government, to the return of his fingerprints and photographs upon an acquittal, is a fundamental right implicit in the concept of ordered liberty and that it is as well within the penumbras of the specific guarantees of the Bill of Rights "formed by emanations from those guarantees that help give them life and substance." *Griswold v. Connecticut*, 381 U.S. 479, 484 (1965).

The court found that the government had not shown any compelling necessity, adding:

---

60The United States Constitution contains no explicit right of privacy, though such a right has been found to exist, with roots in the First, Fourth, Fifth, Ninth, and Fourteenth Amendments, and in the "penumbras" of the Bill of Rights. *Roe v. Wade*, 410 U.S. 479, 508 (1973). Although certain recent state constitutions do recognize such a right, it seems always to be embedded in a general Fourth Amendment-type of Search and Seizure provision, thus casting doubt on its efficacy to provide a "general" right of privacy. See, e.g., 1968 Maryland Constitution, art. 1, § 1; 1968 Hawaii Constitution, art. 1, § 5; 1970 Illinois Constitution, art. 1, § 6.

61The greatest unsettled question is whether Section 10 protects against invasions of privacy by private persons or whether it is directed only against governmental invasions. Though extremely interesting and important, this question is beyond the scope of this comment, because in regard to computerized criminal data systems, we are clearly dealing with state action.

62Under federal constitutional law, "fundamental rights" are accorded a preferred and exceptional status. The United States Supreme Court has held that, "regulation limiting these rights may be justified only by a 'compelling state interest,' and that legislative enactments must be narrowly drawn to express only the legitimate state interests at stake," *Roe v. Wade*, supra note 69 at 728. Use of the "compelling state interest" language in Section 10 suggests that this is the standard by which state invasions of individual privacy are to be tested.


66*Id.* at 217.
We do not believe requiring law enforcement agencies to show a compelling necessity for retention of fingerprints and photographs of acquitted persons places an undue burden on them.\(^6\)

To reach its holding, the court balanced "a right of privacy in the fingerprints and photographs of an accused who has been acquitted . . . against the claim of the state for a need for their retention."\(^7\)

Davidson v. Dill,\(^8\) involved a similar suit by Dorothy Davidson, who was arrested for loitering in Denver, Colorado, and was subsequently acquitted at a trial by jury. She sought alternative relief, either expunging or return of her arrest records. The trial court dismissed her complaint for failure to state a claim upon which relief could be granted. The Colorado supreme court reversed and remanded for trial on the merits, noting:

The issue presented is complex and involves the balancing of the state's interest in efficient law enforcement procedures as against a particular citizen's right to be let alone.\(^9\)

In deciding to remand, the court found persuasive a group of cases holding that:

[A] court should expunge an arrest record or order its return when the harm to the individual's right of privacy or dangers of unwarranted adverse consequences outweigh the public interest in retaining the records in police files.\(^10\)

One commentator points out that a constitutional right of privacy is an affirmative right and is thus far more than a mere right of each acquitted individual to sue for expungement of records pertaining to his arrest.\(^11\) It is in fact an a priori check on the power of the state to keep records containing personal data, or to disseminate those records, unless the state can show a compelling necessity.

Davidson and Eddy were each based on a state court's finding of a paramount right of privacy without the aid of an explicit, general privacy provision in the state's constitution. In Montana, where both the right of privacy and the compelling state interest test are of explicit constitutional status, surely the right can be no less. Thus, there is need to examine any Montana proposal involving collection, retention, and dissemination of personal data with great caution.

\textbf{PRIVACY AND THE CRIMINAL DATA COMPUTER: PROPOSALS}

The following proposals are an attempt to reconcile the competing public interests in law enforcement and privacy, in regard to a centralized Montana criminal data computer system, which will eventually be

---

\(^{6}\)Id. at 218.

\(^{7}\)Id. at 217.


\(^{9}\)Id. at 162-162.

\(^{10}\)Id. at 161.

interfaced with other state and federal systems. The proposals also attempt to take in to full account the state's need to show a compelling necessity at every step of the data handling process, including collection, use, retention, and dissemination.

I. JUVENILE DATA EXCLUDED

No information shall be entered concerning juvenile offenders. Many states, including Montana, require such information to be kept largely confidential, believing that this contributes to the rehabilitation of the youthful offender.82

II. INTELLIGENCE INFORMATION EXCLUDED

No intelligence, analytical, or investigative information shall be entered. The intent here is to exclude unverified data, such as tips, rumors, unsubstantiated allegations, conjecture, and subjective evaluations. Only verified information of public record derived from official criminal justice proceedings may be entered.83

III. SPECIFIED MISDEMEANORS EXCLUDED

No information on misdemeanor drunk or traffic arrests shall be entered. Other minor misdemeanors should also be excluded, and this is a topic for further study.84

IV. DISPOSITION REQUIRED

No arrest data shall be entered until coupled with a disposition. Only dispositions indicating guilt are of legitimate use to law enforcement,85 particularly in light of Montana's constitutional privacy provisions.86 In addition, a person arrested on the type of crime permitted into the computer will generally be in custody or under bail pending trial. Thus, there is no general need for raw arrest information to be entered. If an offender flees the jurisdiction to avoid trial, he then may be entered under the heading of "wanted persons."87 This provision also solves the problem of agencies whose files contain great numbers of arrest entries without dispositions and who are faced with an enormous practical problem of obtaining dispositions.88

V. CONVICTION REQUIRED

Only arrest records followed by a finding or plea of guilty shall be entered. As noted elsewhere in this comment, dispositions of acquittal

82Project SEARCH, supra note 57, Part I at 16-17, excludes juvenile data for this reason. Montana's 1974 Youth Court Act, R.C.M. 1947, §§ 10-1230 (law enforcement records), 10-1231 (youth court records), and 10-1232 (disposition of records), provide for restriction of records involving juvenile offenders until they reach maturity and then for sealing.
83Project SEARCH, supra note 57, Part I at 17, suggests this exclusion.
84"Id.
85See discussion, supra notes 35 and 54.
86See discussion, supra notes 69-71.
87See discussion, infra notes 91-92.
88See supra note 33.
or exoneration have little legitimate use in law enforcement and cannot pass the compelling state interest test.\textsuperscript{89}

VI. ORIGINAL ENTRY

If an arrest record and disposition may properly be entered, that data must be accompanied by other available data on pretrial proceedings, sentence, rehabilitation, and release. Such data not available at the time of the original entry shall be entered when it becomes available. \textquote{Such a file shall be designated a \textquote{criminal history}.}\textsuperscript{90} This is to assure that a \textquote{criminal history} is as complete as possible at any given time.

VII. IDENTIFICATION INFORMATION

\textquote{Identification information}\textsuperscript{91} may be entered only (a) upon proper original entry of a \textquote{criminal history}, or (b) on \textquote{wanted persons}. \textquote{Wanted} shall mean, on certain designated serious felonies,\textsuperscript{92} the person is at large and probable cause exists for arrest, such as where a warrant of arrest has issued. \textquote{Identification information} is necessary upon original entry to establish the identity of the offender whom the original data concerns, as well as subsequent data. This provision is intended to restrict the \textquote{identification information} in the computer to that for which a compelling necessity can be shown. It is also intended to require that once a \textquote{wanted} person is apprehended, the \textquote{identification information} is purged and the computer will contain no more data on him unless and until proper entry can be made under (a).

VIII. FINGERPRINT REQUIREMENTS

No \textquote{criminal history} data may be entered unless accompanied by a fingerprint card bearing designated fingerprints of the data subject. This is necessary to insure proper identification of the subject and all data pertaining to him.\textsuperscript{93}

\textsuperscript{89}See discussion, supra notes 35, 54, and 71-81.

\textsuperscript{90}This label is used here only for convenience.

\textsuperscript{91}Project SEARCH suggests the following identifiers: \textquote{full name, date and place of birth, sex, occupation, race, height, weight, hair color, features, skin tone, identifying marks, FBI number, social security number, any operator's license number, any miscellaneous identifying numbers.} Project SEARCH comments: It should be understood that Social Security and other identifying numbers are included . . . in order to complete or verify individual identifications, and not as a device to permit linkages or data sharing with other information systems.

Project SEARCH, supra note 57, Part I at 16. Privacy-sensitive individuals may well wonder how adequate is SEARCH's disclaimer of \textquote{linkages or data sharing} by use of social security and other such numbers, in view of the \textquote{computer convenience} of such sharing. MILLER, supra note 3 at 60-61.

\textsuperscript{92}There are many possible designations. For example: (a) only serious felonies involving violence against persons; (b) only serious felonies involving violence against persons or property; (c) a list of serious felonies by name which are to be included, such as intentional homicide, sexual intercourse without consent, aggravated assault, kidnapping, and the like.

\textsuperscript{93}Fingerprints remain the best positive identifier. See generally TASK FORCE REPORT: SCIENCE AND TECHNOLOGY, supra note 32 at 77.
IX. Access Limitations

Access to computer information shall be limited to (a) designated law enforcement agencies, (b) approved criminal justice research projects, and (c) the data subject or his properly designated representative. This is intended to place strict controls upon who can obtain the computer information. It might be wise under (a) to establish classes of agencies to receive particular types of information. Under (b), strict regulations should be drawn to control what types of research projects may be approved, how they are to be approved, and strict security controls provided if personally identifiable data is to be used. In general, research projects should require only statistical data. Provision (c) is necessary for instances in which the data subject is unable to appear or act on his own behalf.

X. Notification To Data Subject

The data subject shall be notified at the time of original entry of his "criminal history": (a) of the fact that such entry has been made; (b) of the significance of such entry, including but not limited to classes of persons to whom it may be disseminated, interfacing computer systems through which it may be accessed, and use to be made of it; (c) of the specific, exact and complete contents of his "criminal history"; (d) of his right annually to request and receive an updated copy of his "criminal history"; (e) of his right to challenge inaccurate, incomplete, misleading, or stale data, and the remedies available, including correction, addition, deletion, or total purging of such data; (f) of the method of challenge and of appeal from an adverse decision; (g) of the person responsible, within the agency which controls the central processing unit, for accuracy of the data; (h) of the remedies for violation of his right of privacy; and (i) of the statutory intervals for agency purging of specific types of data.

This notification shall be mailed to the data subject's last known address. Ideally at this time the subject should receive both a pamphlet containing, in very clear and simple language, the standard information outlined above, and a print-out of his own "criminal history." The purpose of this is to provide him with the information he needs to protect his own rights.

XI. Purging

(a) If a subject with a felony conviction has been free from criminal justice supervision for seven years without any subsequent convictions of a nature to be entered in this system, if no prosecution is pending

Sen. Ervin's bill, S. 2963, supra note 52, classifies data and data users. In Montana, because of the relative cost and smallness of the system, this might not be practical. If care is taken to restrict what types of data go into the system, it should also not be necessary.

It is possible that a few worthy projects might need to follow up on particular offenders, as, for example, to study rehabilitation. Most projects requiring individual identification should require consent of those individuals, however; and adequate privacy protections should be provided.
against him, and if he is not a fugitive from justice at the end of that time, his “criminal history” shall be purged. (b) If a subject with a misdemeanor conviction meets the same criteria for a period of four years, his “criminal history” shall be purged. This provision would remove all data from the system on individuals who meet the criteria. It would be effective, however, only if coupled with provisions for purging other systems which have accessed the data, provisions which should be specified in intersystem agreements for exchange or interfacing. Also, provisions must be made to notify agencies which have received print-outs of the data, of a) the purging, and (b) the significance of the purging. Otherwise, the purging may be meaningless. In addition, further study should be given to the question of whether these provisions should apply only to persons with single offenses or to persons with extensive records as well. It may be that the “redemption factor” applies equally or even more to the repeating offender who actually rehabilitates himself. It is also possible, however, that a clear record for a number of years means only that the repeating offender has gained expertise at avoiding detention or conviction. Perhaps type of offense should be considered as well, since some types of offense are known to have a high likelihood of repetition, while others do not. It may be that a provision could be drawn automatically purging data in (b) regardless of prior misdemeanor offenses, but giving some agency discretion in (a) for subjects with specified types of prior offenses.

XII. Negative Answers To Inquires

After data is purged, the data subject may answer all inquiries about his criminal record, whether governmental or otherwise, as if the purged offense had never occurred. This would require that the data subject know of the purging; and provision should be made for official explanation to anyone who, knowing of the record before purging, legitimately questions such an answer.

XIII. Records of Access

The agency which controls the central processing unit shall keep

---

Footnotes:

98 Access by the data subject to his own file might also require use of fingerprints for positive identification.

99 The greatest problem with this approach is that it places most of the burden of protecting these rights upon the individual offender, who is frequently not well-educated and is often indigent. Means should be found to ameliorate this burden as much as is reasonably possible.

90 "Purge" means to remove information from the records of . . . a criminal justice information system so that there is no trace of information removed and no indication that such information was removed." S. 2963, supra note 52, Title I, § 102 (17).

101 It is an open question whether other systems will agree to this or will have statutory authority to negotiate such matters.

102 Objection may be raised that this, like many of the suggestions in this comment, will be costly and will substantially increase the total expense of the program. Rights are frequently expensive to maintain. The alternative is to risk losing them.

103 A number of commentators suggest this approach. See, e.g., The Expungement or Restriction of Arrest Records, supra note 34 at 125.
records of all computer accesses. This is necessary for purposes such as purging and control of improper access.102

XIV. SYSTEM AND PERSONNEL SECURITY

Regulations must be established for security of the central processing unit and of the remote access terminals and for screening and training of all persons who operate such units.103

XV. REMEDIES AND PENALTIES

Criminal penalties and civil remedies must be established for violations and must be substantial enough to serve as deterrents. Civil remedies should include both actual and punitive damages and should be awarded whenever possible with an eye to returning the plaintiff to his situation before the violation. Further study is needed on specific provisions and on the question of negligent as opposed to intentional violations.104

XVI. ADMINISTRATION

A privacy board should be established to set policy, make regulations, conduct hearings, and the like. Again, further study is needed on questions such as: whether there should be one body or two (some proposals suggest both a policy-making body and an administrative body),105 what specific powers the body or bodies should have, and whether these powers should be determined by statute or referred to Montana's general provisions for administrative procedure,106 and under which state department the body or bodies should operate.107

CONCLUSION

The above proposals are intended to highlight areas of concern and to suggest a possible scheme for balancing important conflicting interests. They are not meant to be models for legislative enactment, nor do they exhaust all problems or issues. Many of them are sure to be controversial, to partisans on both sides of the conflict.

102 S. 2963, supra note 52, Title II, Sec. 206(d) would require that this be done.
103 See generally, MILLER, supra note 3 at 239-257.
104 S. 2963, supra note 52, Title III, Sec. 309, provides for maximum criminal penalties of $5,000 fine, five years imprisonment, or both, for "willful" dissemination, maintenance, or use of such information. Sec. 308(e) provides for civil penalties, including a $100 fine for each violation plus actual and general damages, costs, and reasonable attorneys' fees, and for exemplary and punitive damages in specified instances. The civil action is only available after exhaustion of administrative remedies.
105 Project SEARCH, supra note 57, Part II at 16-19; S. 2963, supra note 52, Title III, Sections 301, 302, and 304.
106 R.C.M. 1947, Title 82, Ch. 42, Administrative Procedure Act.
107 Montana's Executive Reorganization Act, R.C.M. 1947, § 82A-104, provides that all "executive and administrative offices, boards, commissions, agencies, and instrumentalities of the executive branch of state government" must operate under the auspices of one of nineteen enumerated departments. On inspection of this list, it is not immediately obvious where a privacy board or commission should be attached. It is doubtful that it should be attached to the Department of Justice, since an important and continuing function would be balancing individual privacy rights against the needs of law enforcement; and with such an attachment, the balance could be lost.
It is imperative that thoughtful attention be paid to these issues, because carelessly drafted legislation which loses the balance can, and predictably will, create a monster. Perhaps the ideal is to do nothing at all; that would surely be better than drifting casually into a “record prison” society, a process which is already well underway.108

As Montana prepares to enter a computerized criminal history system, her citizens would do well to keep alert. As Senator Sam Ervin has commented, freedom, unguarded, slips easily away, and the time for concern is now.

Privacy, like many of the other attributes of freedom, can be easiest appreciated when it no longer exists. A complacent citizenry only becomes outraged about its loss of integrity and individuality when the aggrandizement of power in the Government becomes excessive. By then, it may be too late. . . . Nor should we wait until there is such a threat before we address this problem. Protecting against the loss of a little liberty is the best means of safeguarding ourselves against the loss of all our freedom.109

108See generally MILLER, supra note 3, and Westin, supra note 18.