Volume 54 | Number 4 Article 3

4-1-1976

Privacy and Record Keeping: Remedies for the Misuse of Accurate Information

Peter N. Swan

PRIVACY AND RECORD KEEPING: REMEDIES FOR THE MISUSE OF ACCURATE INFORMATION

PETER N. SWAN†

Modern societies are indisputably information-intensive. This is an understandable consequence of telecommunication networks that span continents and oceans, commercial practices that rely heavily on credit, welfare economics that impact upon millions, research facilities, and industrial processes that create and require huge quantities of data. The ability to process and communicate information permits tremendous efficiencies and technological progress, but it also creates vulnerabilities and opportunities for abuse.

Tort law has evolved a sizable jurisprudence for handling untrue utterances and publications that are damaging to reputation. The remedies for invasion of privacy fostered by Warren and Brandeis have dealt in limited measure with accurate but harmful disclosures.[1] Yet American law has never developed a coherent body of law to handle all forms of unauthorized use of accurate information. Indeed, a sizable part of the problem is the very determination of what is "authorized" and what is not.

This article will examine the various tort principles through which information misuse claims can be analyzed and resolved. It will demonstrate that non-tort law approaches, especially statutory remedies, are often possible. Tort law will be examined for incompleteness and for areas of potential expansion. An effort is made to gauge its effectiveness to cope with present-day problems and to assess the wisdom of its bounds and limits. Existing legislative solutions are discussed. A proposed model statute covering the specific problem of maintaining criminal justice data is developed and defended. The rogues gallery of villains in this piece includes indifferent custodians, spiteful detectives, greedy competitors, and criminals. The victims range from borrowers of money and seekers of licenses through ex-convicts and mental patients.

---

† Professor of Law, The University of Oregon School of Law.

1. *See* Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

COMMON LAW TORT THEORIES

Tort theories for misuse of information include intentional behavior, negligence and, arguably, strict liability.[2] Persons may misuse data through motives of profit or spite, or they may simply be indifferent to the consequences to the data subject. Thus, defendants may be data custodians, data users, chance recipients, or persons who discover, extract, or revive basic facts.

The numerous cases finding liability against harassing creditors represent one variety of an intentional tort theory of recovery. The earlier cases were the precursors of the tort of intentional infliction of emotional distress.[3] Other cases involving bill collectors, in which repetitiveness or vindictiveness were not so evident, were arguably decided under theories of invasion of privacy by publicity.[4] In the former cases, the use of the information itself was ancillary to the behavior and

---

2. Strict liability has been utilized in defamation cases when the defendant neither knew of the plaintiff nor intended to defame him. *See* Smith, *Jones v. Hulton: Three Conflicting Judicial Views as to a Question of Defamation*, 60 U. PA. L. REV. 365, 371 (1912). Similarly, liability for defamation was traditionally visited upon republishers regardless of their lack of intent or fault. *See, e.g.*, Corrigan v. Bobbs-Merrill Co., 228 N.Y. 58, 126 N.E. 260 (1920) (book publisher). *But see* Balabanoff v. Fossani, 192 Misc. 615, 81 N.Y.S.2d 732 (Sup. Ct. 1948) (large newspaper vendor). *See generally* Painter, *Republication Problems in the Law of Defamation*, 47 VA. L. REV. 1131 (1961). It could be argued that even if accurate information pertaining to plaintiff which would offend the sensibilities of the ordinary man is disseminated without fault or neglect, the disseminator should be liable by analogy to the republication concept. This argument is not likely to prevail: a truly accidental dissemination should not be actionable. Secondly, most disseminations are intentional, though there may well be difficulty in showing they understood or knew to a "substantial certainty" that harm would ensue from the disclosure. Thirdly, some situations may arise where the disclosure is, indeed, intentional, but is motivated by a reasonable, yet erroneous belief that disclosure is privileged. *See* text accompanying notes 13-14 *infra*. On the other hand, some of the reasoning underlying the recent erosion of republishers' liability, viz. that a more culpable and responsible defendant is available, is not necessarily appropriate to the accurate information cases. In the latter, the author or collector of the data is often privileged. It is the custodian or disseminator (the republisher) whose act of transmittal and publication is the first (and perhaps the only) harmful and unprivileged act. This does not resolve the ultimate question of who should bear the loss, but it does permit the analysis to focus squarely on the disseminator.

The recent case of Gertz v. Robert Welch, Inc., 418 U.S. 323 (1974) proscribed strict liability in defamation actions and this proscription was recognized in a false-light defamation case, Drotzmanns, Inc. v. McGraw-Hill, Inc., 500 F.2d 830 (8th Cir. 1974). This may well preclude the application of strict liability principles to accurate information cases since if *un*true publications derive partial shelter from first amendment concerns, presumably accurate publications would be at least as deserving of protection from liability without fault.

3. *See, e.g.*, Duty v. General Fin. Co., 154 Tex. 16, 273 S.W.2d 64 (1954).

4. *See, e.g.*, Trammell v. Citizens News Co., Inc., 285 Ky. 529, 148 S.W.2d 708 (1941) (newspaper notice of amount owing); Brents v. Morgan, 221 Ky. 765, 299 S.W. 967 (1927) (signboard publicizing amount owing).

motives of the collector.[5] In the latter cases, however, it was seemingly the purpose to which the information was applied or the manner of its employment that justified liability.

Another type of intentional tortfeasor is the person who commits or threatens to commit extortion. Under most circumstances, this is a criminal act punishable under criminal law. No appellate decisions can be discovered in which the mere threat to disclose (whether or not successful in getting the "hush money") has been held to be a tortious misuse of information. If the blackmailer's bluff is called, however, and he or she then discloses the information, this could constitute "misuse." If the information is intimate and theretofore unknown, a disclosure to the public generally, or at least to a substantial number of people, would constitute an actionable invasion of privacy. If the information was not personally embarrassing but was merely a fact that would be prejudicial when disclosed, the privacy theory does not apply.[6] Nevertheless, one is left with a feeling that such a disclosure serving no societal function should be redressable. Perhaps both the blackmailer who carries out his threat and the spiteful person who discloses without a prior extortion attempt should be reached under a prima facie tort theory.[7]

The governmental agencies that have custody of the greatest amount of potentially prejudicial accurate information are the law enforcement agencies. Leaving aside the negligibly small number of instances in which vindictiveness may be involved, there are still believed to be a sizable number of instances in which information is leaked through carelessness, misguided notions of public responsibility, or the return of favors to private investigators or friends.[8] These disclosures,

5. This is especially true when the data concerning the amount allegedly owing was only communicated to the plaintiff or his agents or family. Excessive or repetitive communication of the information to the alleged debtor's employer may also fit this classification.

6. The requirement that the disclosure have concerned "intimate facts" has been broadened somewhat and the test now is whether the disclosed information would have offended a person of ordinary sensibilities had such information pertained to such a person. *See* Samuel v. Curtis Publishing Co., 122 F. Supp. 327 (N.D. Cal. 1954). The broader test would probably encompass financial circumstances that were unique to the individual, even though personal emotions, family relationships or physical behavior need not have been involved.

7. *Cf.* Tuttle v. Buck, 107 Minn. 145, 119 N.W. 946 (1909) (predatory competition with vindictive motive). For a criticism of the publicity variety of the invasion of privacy tort see Kalven, *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 LAW & CONTEMP. PROB. 326, 333-37 (1966).

8. In the author's experience, private investigators sometimes assure clients that they have "reliable inside sources" in government agencies that can expeditiously provide recorded data to the investigator. At a hearing before the House Judiciary Committee of the Oregon Legislature in 1973 (H.B. 2470), a former police department employee tes-

both negligent and intentional, might often be redressable under an invasion of privacy theory if widespread publicity is given the leaked data. If the material is released only to a particular person in a position to prejudice the file subject, the publicity-privacy theory becomes less tenable, and the prima facie tort or statutory remedies must be utilized.[9]

Defenses

There are instances, however, when even a spiteful disclosure could support societal purposes. The legally disinterested person who reduces or eliminates the inheritance of a putative heir by revealing the whereabouts of the missing true heir is, regardless of motive, helping the law achieve the purpose of predictable and fair succession of wealth. Similarly, the person who comes forth with compromising facts about a political figure, though acting from base motives, may nevertheless further society's interest in having the most able and least vulnerable persons attain or hold office. If the analysis proceeds upon the theory of a qualified privilege, malicious motives should destroy the privilege even in such cases. But the qualified privilege notion derives principally from the law of defamation. There, the maliciousness is arguably interrelated with the knowing promulgation of an untruth. In other words, it may be that the courts have focused on scienter instead of on just the motive for disclosure.[10] If motive *is* the sole desideratum in the qualified privilege cases, the notion could be transplanted to the accurate information cases, but this would seem counterproductive.[11]

To the extent such intentional disclosures are actionable, redress should lie against the persons paid or bribed to divulge or make accessible the information within their control as well as against the person desiring disclosure. Thus the bank officer or records clerk through

---

tified that he witnessed a fellow officer, as a favor to a friend who managed a motel, repeatedly check the wanted persons, stolen car, and criminal record files concerning certain motel customers.

9. Perhaps false-light theories of defamation could also be employed. Publicity-type invasions of privacy have generally required some public or relatively widespread disclosure. *See* Santiesteban v. Goodyear Tire & Rubber Co., 306 F.2d 9 (5th Cir. 1962). *But see* Simonsen v. Swenson, 104 Neb. 224, 177 N.W. 831 (1920) (per curiam) (no liability since disclosure privileged); Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 MICH. L. REV. 1091, 1157-58 (1969). For statutory remedies see text accompanying notes 57-83 *infra*.

10. *See* Iverson v. Frandsen, 237 F.2d 898 (10th Cir. 1956); Stationers Corp. v. Dun & Bradstreet, Inc., 62 Cal. 2d 412, 398 P.2d 785, 42 Cal. Rptr. 449 (1965).

11. *Cf.* Craig v. Wright, 182 Okla. 68, 76 P.2d 248 (1938) (alleged defamatory statement found to be true); W. PROSSER, LAW OF TORTS 794-96 (4th ed. 1971).

whom the spiteful actor gains the damaging information should be liable if he or she knowingly breached a confidence or violated a statutory restraint. Private investigators, journalists, researchers and others who collect, collate and analyze raw or incomplete data should not be liable so long as they had no initial control or custody of the information and disclosed it to no one except their client or employer.[12]

When the information is contained in or derivable from the records of a federal or state agency, the Freedom of Information Act or its state counterpart, will be relevant as a defense for the disclosing custodian. Here the scope of the exception for confidential material will likely be the determinative issue. If a subjective test is used, focusing upon the *attitude* of the subject toward the information supplied to the agency, more data will be within the exemption. On the other hand, an objective test would eliminate more data from the exemption.[13] Problems arise when the information is already disclosed as a result of an agency employee's disregard or misconstruction of the exemption provision. Since it is too late to enjoin disclosure, the question becomes whether damages be recovered from the agency or, from the individual employee. The disclosure would be deliberate (since that was a part of the employee's job) but not necessarily "intentional" in the sense of an intentional tort.[14] Assuming the misconstruction of the exemption was negligent, the question of immunity arises. If the employee were not a high-level policymaker, the absolute immunity of *Barr v. Matteo*[15]

12. This is so even though the investigator's name and the identity of his sources (if human) would have to be disclosed. *Cf.* Branzburg v. Hayes, 408 U.S. 665 (1972) (5-4 decision). In Pearson v. Dodd, 410 F.2d 701 (D.C. Cir.), *cert. denied*, 395 U.S. 947 (1969), the court held the intrusionary methods of those who acquired Senator Dodd's papers for clandestine copying and return would not make columnist Drew Pearson liable for an intrusionary invasion of privacy. This was so even though the defendant knew how the copies of the documents had been obtained when they were presented to him. Defendant was held not liable on an independent count concerning a publicity-type invasion of privacy as his publication was privileged. *Id.* at 703-06.

13. *See, e.g.*, Wine Hobby USA, Inc. v. IRS, 502 F.2d 133 (3d Cir. 1974). *See also* National Parks & Conservation Ass'n v. Morton, 498 F.2d 765 (D.C. Cir. 1974); Annot., 21 A.L.R. Fed. 224 (1974).

14. Of course, one can imagine a situation where a public employee disclosed the information pursuant to a request under the Freedom of Information Act *knowing* that one of the exemptions applied and knowing, or at least suspecting, that the plaintiff would be injured by its release. This would be an intentional violation of the Act.

For an instance where statutory bases for exemption from disclosure under the Act have been enumerated in detail see 5 U.S.C.A. § 552(b)(7) (Supp. 1976) ("investigatory records compiled for law enforcement purposes"). *See generally* Ellsworth, *Amended Exemption 7 of the Freedom of Information Act*, 25 AM. U.L. REV. 37 (1975).

15. 360 U.S. 564 (1959) (absolute privilege in libel action for acting director of federal Office of Rent Stabilization).

should not be available. The availability of qualified immunity to the employee will usually depend upon statute.[16] The further question exists whether there was a waiver of sovereign immunity were the agency itself joined as a defendant. Waiver statutes frequently exclude liability for defamation and for intentional torts.[17] Assuming the information disclosed is true, it cannot be said that plaintiff is suing in defamation; yet one suspects the legislature was attempting to exclude informational torts generally, and a hasty amendment might be expected if courts found a lack of immunity. Protectors of trade secrets and personal privacy might well suggest that this is an area in which the government should be open to liability since the possibilities for abusing its custodianship of coercively collected accurate information are manifest.[18]

CREDIT BUREAUS, MEDICAL RECORDS, AND CUSTODIANS

The nongovernmental entities that have custody over large amounts of potentially damaging data are credit bureaus and investigative reporting agencies. The bureaus, whether commercial[19] or cooper-

16. *See, e.g.*, Elder v. Anderson, 205 Cal. App. 2d 326, 23 Cal. Rptr. 48 (5th Dist. 1962); *cf.* Carter v. Carlson, 447 F.2d 358 (D.C. Cir. 1971) (civil rights case), *rev'd sub nom.* District of Columbia v. Carter, 409 U.S. 418 (1973).

17. *See, e.g.*, 28 U.S.C.A. § 2680(h) (Supp. 1976) (libel). *But see* Quinones v. United States, 492 F.2d 1269 (3d Cir. 1974) (claim for *negligent* maintenance of personnel records prejudicial to former employee's job prospects *not* within exemption for libel under Federal Tort Claims Act). *See also* Appendix § 14.

18. *See* Doe v. McMillan, 412 U.S. 306 (1973); Turner v. Reed, 538 P.2d 373 (Ore. App. 1975). In *Turner*, the court held "public records where the only interest in confidentiality is to protect public officials from criticism of the manner in which they have discharged their public duties [to be per se available for public inspection]" and added "[c]itizens are entitled to inspect public records to learn what their government is doing—this means learning of government's possible shortcomings, not just government's successes." *Id.* at 381. For a discussion of government agencies selling data for commercial mailing lists, see Hey, *How many chinks in your privacy wall?*, Christian Science Monitor, Nov. 5, 1970, at 11, col. 1. For a general discussion of mailing lists, their economics and their potential abuses, see SECRETARY'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYSTEMS, HEW, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS 288-97 (1973) [hereinafter cited as HEW REPORT].

19. The growth of commercial credit bureaus has been nothing short of dramatic. Associated Credit Bureaus, Inc., an organization with around 1900 credit bureau members, estimated its members maintained about 110 million files in 1969. Its credit bureau members do not compile investigative reports. They do provide credit reports to banks, retail merchants and finance companies. Retail Credit Company is the largest investigative report preparer in the country (preparing nearly eighty-five percent of all such reports). It is the corporate parent of Credit Bureau, Inc., which in turn does own conventional credit bureaus. Thus there exist financial and directive interconnections between the two functions but they are most often accomplished in separate physical locations and with different personnel, employed by separate entities. Telephone interview with Barry Connelly, Vice President of Associated Credit Bureaus, Inc., in Hous-

atively owned,[20] are both the collectors of the information and the custodians of it once compiled. This presents some doctrinal problems. First, the majority of the information gathered, *e.g.*, tenure of employment and tax liens, is not per se confidential. Secondly, it could be argued that having taken the effort to collect the information from disparate sources and to compile it, the credit bureau may dispose of it as if it had a proprietary interest. Thirdly, the disclosures of a credit bureau have traditionally enjoyed a qualified privilege in defamation law, and, by analogy, it could be argued that accurate disclosures to members or clients with an asserted need to know should enjoy a similar privilege.[21]

The probability of inaccurate or distorted information being included in the compilation has been documented,[22] as has the danger of dissemination to those not having even an attenuated need to know.[23] Apart from the erroneous information problem is what could be called the "saliency factor" or the "oracle syndrome." However reliable the original source of information may have been, the heavy reliance on automated data processing devices and the related high cost of data storage lead inevitably to synopsizing, highlighting, collapsing, compacting, and terseness. This frequently results in a qualitative deterioration of the data in terms of cybernetic value. The potential for an unjustifiably damaging impact is exacerbated by the tendency of laypersons to hold the computer and its output in awe as infallible and omniscient.[24]

---

ton, Texas, Apr. 11, 1975.

For a brief description of the meteoric rise of TRW-Credit Data Corporation (which is not an Associated Credit Bureaus member), see A. WESTIN & M. BAKER, DATABANKS IN A FREE SOCIETY 132-35 (1972).

20. *See, e.g.*, London Ass'n for Protection of Trade v. Greenlands, Ltd., [1916] 2 A.C. 15.

21. *See* Bartels v. Retail Credit Co., 185 Neb. 304, 175 N.W.2d 292 (1970) (privilege lost by recklessness); Annot., 30 A.L.R.2d 776 (1953); *cf.* Annot., 40 A.L.R.3d 1049 (1971). *See also* Kansas Elec. Supply Co. v. Dun & Bradstreet, Inc., 448 F.2d 647 (10th Cir. 1971) (no first amendment privilege for retail credit bureau).

22. A. MILLER, THE ASSAULT ON PRIVACY 84-87 (1971).

23. *Id.* at 87-88. *But see* A. WESTIN & M. BAKER, *supra* note 19, at 255, 440 (suggesting that computerization per se has little to do with information sharing with government agencies).

24. Alan Westin and Michael Baker have determined that overreliance on computer print-outs is no more frequent or aggravated than overreliance on manually recorded conclusions and summaries. A. WESTIN & M. BAKER, *supra* note 19, at 259-64. Similarly they contend that coding data for computer processing did not lead "to any greater misuse of shorthand notations than was present in the manual era." *Id.* at 266. They also believe that computerized systems, being susceptible of rapid updating, would show an increase in accuracy. *Id.* at 300. The trend is definitely toward computerizing and networking the files. *See* A. MILLER, *supra* note 22, at 90-93. For a good general discussion of the sociological impact of computerized records see Comment, *The Com-*

Allowing such output to reach others to whom the original sources are not available can be classified either as a material untruth by creating a false light or as the misuse of accurate (so far as it goes) information. The exact description might be regarded as nothing more than a semantic problem were it not for the common law's reluctance to redress the latter situation.

Moreover, even if the recipient of the credit report receives a valid impression based on accurate computer input, damage to the file subject could result.[25] If the recipient has a real need to know,[26] it can be convincingly argued that society's needs in the capital, underwriting and employment markets are superior to the individual's desire that the past remain secret and are even superior to the need to rehabilitate criminals, bankrupts and misanthropes. However, the dissemination can be overly broad, especially when disclosed to persons or entities that do not have an immediate potential of entering into significant economic or therapeutic relationships with the file subject. To suggest that no damage would flow from such revelation since no economic consequences are probable is to disregard the dignitary aspects of the action for invasion

---

puter Data Bank-Privacy Controversy Revisited: An Analysis and an Administrative Proposal, 22 CATH. U.L. REV. 628, 636-42 (1973).

25. This assumes that the sources of the data input to the file were accurate ledgers and records, fair-minded individuals with good perceptions and memories, and unequivocal circumstantial evidence. Obviously such idealized prerequisites are seldom satisfied and this difficulty is not unique to credit or investigative reporting. Nevertheless, it should make one chary of making conclusive human decisions based solely on past history.

In order not to compound the potential qualitative weaknesses of input, certain minimum safeguards are required. As one study group suggested, record-keeping organizations should adhere to the following fundamental principles:

> °There must be no personal-data record-keeping systems whose very existence is secret.
>
> °There must be a way for an individual to find out what information about him is in a record and how it is used.
>
> °There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
>
> °There must be a way for an individual to correct or amend a record of identifiable information about him.
>
> °Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

HEW REPORT, *supra* note 18, at 41.

26. The Fair Credit Reporting Act, 15 U.S.C. § 1681b (1970), lists the following as permissible recipients of consumer reports (which may include investigative material): persons reasonably believed to require the data for (a) entering into a credit transaction involving the file subject; (b) employing the file subject; (c) underwriting insurance involving the file subject; (d) conferring a governmental license as to which the applicant's (file subject's) financial status is relevant as a matter of law; (e) entering into a "business transaction" "involving" a file subject.

of privacy. Emotional distress or the deprivation of the individuality[27] of the file subject is suffered merely by the awareness that such matters are now known to third persons.[28] In these overly wide dissemination situations the invasion of privacy concept is slightly but not fatally attenuated. The information has either been selectively disclosed by the subject or is lying dormant in the public domain, needing only to be identified with the subject and republished to have a fresh impact on the subject.[29] The selective disclosure is often in a context of economic necessity; thus it does not strain the concept too far to suggest that the data is as private as the subject can realistically make it. The public domain issue is more difficult to resolve in favor of the data subject since society has traditionally enjoyed access to accurate reportage of historical fact. Yet, the further in the past the event or transaction occurred, the utility of allowing public dissemination becomes correspondingly less. If the dissemination is to a limited number of persons as opposed to the general public, the utility may be even less.[30]

The next most common types of dossier or personal data compilations are medical records. These compilations have some similarity to credit records in that there are valid reasons for maintenance of the data and for dissemination on a need to know basis. On the other hand, there is perhaps a greater tradition of confidentiality in the medical industry than in the credit industry. Even the type of treatment history data that does not qualify as a *communication* from the patient to the

27. *See* Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U.L. REV. 962 (1964).

28. In the areas of credit experience, prior employment and medical treatment, it is apparent that the events described were never wholly intimate in the sense that they were known only to the data subject. Nevertheless, the number of persons who knew was limited and they obtained their knowledge through the necessities of the occurrence. The data subject's steeling himself for such a limited disclosure in no way suggests comfort with or adaptability to wider dissemination.

29. *Cf.* Briscoe v. Reader's Digest Ass'n, 4 Cal. 3d 529, 483 P.2d 34, 93 Cal. Rptr. 866 (1971) (criminal record); Melvin v. Reid, 112 Cal. App. 285, 297 P. 91 (4th Dist. 1931) (earlier career as a madam).

30. Superficially, it could be argued that plaintiff's injury will also be commensurately less. There are two difficulties with this position. If the harm is viewed as a dignitary injury, there need be no necessary quantitative relationship to the number of recipients. (Note the anomaly here: for defamation where the law attempts to redress reputational harm, disclosure to a single person is sufficient; for invasion of privacy where dignitary, subjective victimization is arguably what is to be redressed, disclosure to a substantial number of persons is often required.) Secondly, if the "wrong" few people received the disclosure (*i.e.* those with power directly or indirectly to withhold benefits to the subject) they could inflict more injury than thousands of disinterested or "powerless" recipients. On the other hand, it is conceivable that such key people would be most likely, if anyone could, to demonstrate a need to know.

physician[31] may be treated by the record custodian as unavailable to third parties absent consent by the patient.

CRIMINAL JUSTICE DATA

Criminal records differ from credit records in that law enforcement agencies rather than private companies generate and maintain them. Here the need to know lines are hard to draw. Those individuals immediately concerned with the apprehension of suspects, the prosecution and sentencing of criminal defendants, and the detention, parole, probation and rehabilitation of prisoners obviously have such a need with respect to many matters in the person's file. The need is less obvious, however, when the data is shared with out-of-state law enforcement agencies, with members of the agency who have a personal as opposed to a functional interest, and with government officials acting in a political capacity.[32]

A substantive philosophical issue is whether mere constraints on dissemination are sufficient or whether, additionally, there should be internal constraints based on a genuine need to know. Law enforcement professionals point out that intentional, internal violations are extremely rare and need-to-know monitoring (as opposed to training and inculcation of access standards) would be disproportionally expensive and inefficient. They argue that if constraints are appropriate, it is quite sufficient to place constraints on dissemination. These arguments do not adequately deal with corrupt personnel or those who disseminate data through unconventional (and thus unaudited) channels. Of course, even internal access audit procedures can be circumvented by a determined and skillful expert, but such procedures would at least draw attention to most of those who achieve access without any plausible need to know.

Potential employers present a special case with countervailing social policies at play. The goal of rehabilitation and the need to assimi-

31. Such communications are, in many jurisdictions, subject to an evidentiary privilege. *See, e.g.*, ORE. REV. STAT. § 44.040(d) (1974) (applies to all information acquired in attending a patient but for civil actions only). Where a statutory or common law basis for the privilege does not exist, the doctor's professional ethics may not be enough to justify refusal to divulge. *See* Quarles v. Sutherland, 215 Tenn. 651, 389 S.W.2d 249 (1965). If the information is not sought in a litigation context, no evidentiary privilege would apply.

32. Consider the situation of a governor who is commander in chief of the state police but may wish to study a person's file for purely political reasons or for hybrid reasons such as appointment to a government job in which discretion and honesty are vitally important.

late criminals who have fulfilled their sentence into mainstream society are vitally dependent upon employment. It can certainly be argued that having paid his debt to society the "ex-con" should be able to make a fresh start free from suspicion and intolerance. Yet the rehabilitation process is notably fallible, and some forms of employment may provide too great a temptation to engage in recidivistic conduct. The interests of the potential employer, other employees, and the public may require that certain employment be available to ex-convicts only if the employer is willing and fully informed.[33]

Another special case centers around efforts to induce more care by drivers through more directly reflecting the costs of the injuries they inflict in insurance rating categories. Here, convictions for drunk driving, reckless driving, manslaughter with a vehicle, and related offenses should be transmitted to the driver's liability insurer.[34] In jurisdictions having automatic license suspension or revocation for chronic offenders, this information should also be sent to the appropriate state licensing authority.

When it is unclear that the criminal justice data is actually erroneous, but it can be shown that it was gathered or adduced without minimum due process protection to the file subject, dissemination should be prevented. This is not to say that such data may not be generated or recorded in the first instance,[35] but rather it should not be

33. See Appendix §§ 4(3)-(4). To the extent that parolees are seeking jobs, it cannot even be accurately said that they have "paid" their debt to society: at best they are still "paying." However this retributive attitude appears to be receding in favor of the rehabilitative approach, so notions of a "balance owing" may well be inappropriate. If, on the other hand, one's criminal past is *not* a job-related concern, perhaps confidentiality statutes should expressly allow ex-convicts to answer negatively to questions about criminal records on job applications and should prohibit employment discrimination based on discovery of a criminal past. In Tosh v. Buddies Supermarkets, Inc., 482 F.2d 329 (5th Cir. 1973), the court condoned an employer's acquiring (from a friend in the police department) copies of criminal records of troublesome union organizers and posting them to be seen by other employees. The court reasoned this was consistent with minimizing risks to store personnel.

34. Presumably, one or more convictions for violating the vehicle code (at least provisions which pertain to safety) will eventually result in a less desirable rating category for automobile insurance purposes. The theory assumes that past behavior is indicative of future behavior and that the laws do indeed proscribe unsafe conduct. Given these assumptions, the new rating will require higher premiums, thus partially internalizing the costs of the insured's statistically more injurious behavior. For a discussion of premium cost allocation techniques not based on individual experience see Morris, *Enterprise Liability and the Actuarial Process—The Insignificance of Foresight*, 70 YALE L.J. 554, 567-69 (1961).

35. *Cf.* Wisconsin v. Constantineau, 400 U.S. 433, 436 (1971) (publication of no-sale drunk without prior hearing); Joint Anti-Fascist Refugee Comm. v. McGrath, 341 U.S. 123, 126 (1951).

disseminated beyond those needing to know for law enforcement purposes. This would include "intelligence data" that is primarily subjective or investigatory and deductive, and frequently contains or is based on hearsay. If sufficient safeguards are not present with regard to physical security, remote access, unaccounted for copies, loss of saliency, and encryption of transmissions in computerized systems, many feel it is best to keep intelligence material outside of the computerized system altogether.[36]

Finally, there is the extremely difficult problem of access to records and intelligence reports for national security purposes. No completely satisfactory solution to the tension between personal privacy and national security has emerged, but it is apparent that national security interests usually prevail. If a serious national security risk is involved, federal agents will most certainly conduct their own investigation if they are denied access to existing records and reports of state agencies. Efficiency in both time and taxpayer cost would dictate the elimination of such redundancy. On the other hand, since the accuracy of investigative data may be open to doubt, redundancy would improve reliability. Still another possibility is that, faced with the necessity of an independent investigation, federal agents will reappraise the risk and forego the investigation itself, with the possible exception of prospective surveillance.

If the records are criminal records in the custody of a state law enforcement agency, the problem is essentially one of federalism.[37]

36. *E.g.*, IOWA CODE ANN. § 749B.8 (Cum. Supp. 1976); S. 2963, 93d Cong., 2d Sess. § 208 (1974); *see* Appendix § 12. Some of Westin's research indicated (though not unequivocally) that the majority of data systems in his sample kept narrative, sensitive and subjective data off the computer and in manual files instead. A. WESTIN & M. BAKER, *supra* note 19, at 424-27.

The use of information heard or recorded by means of telephone wire taps is beyond the scope of this article. Suffice it to say that law enforcement and national security wire taps are covered by the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-20 (1970). Civil redress for the person whose communication was unlawfully intercepted, used or disclosed is provided against the tapper, user or discloser for actual damages or liquidated damages ($100 for each day of violation or $1000) whichever is greater. *Id.* § 2520.

For a general discussion of governmental wiretapping see Glasser & Schwartz, *Your Phone is a Party Line*, HARPERS, Nov. 1972, at 106. *See also* Simpson v. Simpson, 490 F.2d 803 (5th Cir. 1974) (spouse-instigated wiretap of own spouse, not prohibited by Omnibus Crime Control Act).

37. Where an individual's personal expectations of privacy are involved, the fourth amendment will offer protection agasint warrantless searches by federal agents concerned with domestic security. *See* United States v. United States District Court, 407 U.S. 297 (1972) (domestic wiretap); Burrows v. Superior Court, 13 Cal. 3d 238, 529 P.2d 590, 118 Cal. Rptr. 166 (1975) (bank surrendered depositor's records to police). But when intelligence gathering concerning foreign powers is involved, it appears that a warrant

Absent a federal or a state statute, the state officials could either comply with or refuse the federal agents' requests as they saw fit. If, in such a situation, the federal agents obtained a subpoena duces tecum, the disclosure would have to be made. If there were a state statute forbidding such disclosure, the state officials' refusal to obey the subpoena should be sheltered. But a federal statute compelling such disclosure with or without a warrant or subpoena would preempt the state law, and the officials would have to comply.[38]

Keeping compilations from news reporters raises first amendment questions. Of course, the press is not foreclosed from all access since they can observe the daily police "blotter"[39] and judicial docket entries,

---

will not be required if the agents are acting within the scope of their delegated authority from the President. *See* United States v. Butenko, 494 F.2d 593 (3d Cir.), *cert. denied*, 419 U.S. 881 (1974); United States v. Brown, 484 F.2d 418, 425-56 (5th Cir. 1973). However, the District of Columbia Court of Appeals in Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975), held that a warrant was required to tap the telephones of members of the Jewish Defense League which opposed the emerging United States-Russian detente notwithstanding a presidential directive concerning foreign intelligence gathering for the protection of national security. When the file subject does not suffer an invasion of his own dwelling, car, or privacy envelope (*e.g.*, Katz v. United States, 389 U.S. 347 (1967); North v. Superior Court, 8 Cal. 3d 301, 502 P.2d 1305, 104 Cal. Rptr. 833 (1972)), but rather suffers access to personal data in the hands of another, it is doubtful that he can apply his constitutional right to the obtaining of information from the custodian. *Cf.* California Bankers Ass'n v. Shultz, 416 U.S. 21, 52-53, 55 (1974) (fourth and fifth amendments). This is so even though the custodian might have suffered a deprivation of his own rights under the fourth amendment (*e.g.*, Daniel Ellsburg's psychiatrist).

38. U.S. CONST. art. VI; *see* Union Bridge Co. v. United States, 204 U.S. 364 (1907).

39. *See* Appendix § 4(5). The police blotter would reflect arrests made on that day in that precinct. Thus the information derivable from the blotter would not be cumulative. Compiling a record of any one individual's arrest history would therefore require daily checks and an ad hoc compilation by the investigator (journalist). Although this method is less efficient than present methods, verification of alleged harassment (*e.g.*, by unjustified, successive "rousts" or arrests) could still be accomplished. Moreover, the victim could subpoena his compilation for any proceeding before a police review board or court so the records would not be suppressed in any formal challenge to such harassment. *See* Appendix §§ 4(2)(a), 10(1)-(4). Of course, if a group of law enforcement agents conspired to carry out oppressive tactics and protect themselves, they would not make records in the first place; but this slight risk is present with or without press access to individual criminal histories. Department of Justice policy presently does not permit disclosure of prior convictions of a criminal defendant or a civil party litigant or civil witness. *See* 28 C.F.R. §§ 50.2(b)(4), (c)(2) (1975). The Executive Director of the American Civil Liberties Union is even against press access to the daily police blotter. *Hearings on H.R. 13315 Before Subcomm. No. 4 of the House Comm. on the Judiciary*, 92d Cong., 2d Sess., ser. 27, at 167 (1972).

Even now, not all "public," *i.e.* governmental, records are subject to disclosure. In Oregon, for example, if Corrections Division officials can persuade a court that the public interest in confidentiality clearly outweighs the public interest in disclosure, prison and parole records need not be disclosed. ORE. REV. STAT. § 192.500(2)(d) (1974). See Turner v. Reed, 538 P.2d 373 (Ore. App. 1975) (subjective advisory or

attend trials, and access summary records pertaining to prison releasees or escapees. Wanted and missing persons data can be publicly disseminated. There may be objections to making such data confidential thereafter. One answer to this is that there is a substantial difference between a single item of current newsworthiness and an entire compilation that may go back twenty years or more. Another objection may be that such restraints on access will cause newspapers, credit agencies, and employment agencies to create their own data banks of unsupervised reliability. This seems speculative at best since the collection process would be expensive; on the other hand, title insurance companies do just that with excellent efficiency and reliability.

The Supreme Court in *Cox Broadcasting Corp. v. Cohn*[40] has spoken broadly on the subject of freedom of the press in the criminal justice context. *Cohn* involved a television newscast report identifying a rape-murder victim. A Georgia statute prohibited such disclosures, and the father of the deceased brought an action for invasion of *his* privacy. Because the newsman had obtained the information legally—by examining the indictment during the course of the trial—the statute was attacked on first amendment grounds.[41] The Court held the statute invalid but expressly declined to "address the broader question whether truthful publications may ever be subjected to civil or criminal liability consistently with the First and Fourteenth Amendments, or . . . whether the State may impose sanctions on the accurate publication of the name of a rape victim obtained from . . . judicial records . . . open to public inspection."[42] Having carefully limited its holding, the Court then added that "[t]he commission of crime, prosecutions resulting from it and judicial proceedings arising from the prosecutions . . . are without question events of legitimate concern for the public and consequently fall within the responsibility of the press to report the operations of government."[43] While this is undoubtedly true with respect to current news and statistical studies of law enforcement, it does not necessarily follow that *all* such material is *forever* protected. The Court next said, however, in expansive dictum:

> By placing the information in the public domain on official court records, the State must be presumed to have concluded that

evaluative material shielded from disclosure but objective information generally not shielded).

40. 420 U.S. 469 (1975).
41. *Id.* at 474.
42. *Id.* at 491.
43. *Id.* at 492.

> the public interest was thereby being served. Public records by their very nature are of interest to those concerned with the administration of government, and a public benefit is performed by the reporting of the true contents of the records by the media. The freedom of the press to publish that information appears to us to be of critical importance to our type of government in which the citizenry is the final judge of the proper conduct of public business. In preserving that form of government the First and Fourteenth Amendments command nothing less than that the States may not impose sanctions for the publication of truthful information contained in official court records open to public inspection.[44]

This suggests that the Court believes "once public, always public." Yet it would not seem inconsistent for a state to "conclude" that criminal justice information should be public only in relevant segments and at relevant times.[45] Also, the state might take a different view of balancing the continuing privacy interest of a live file subject as contrasted with the more attenuated "one-shot" interest of a parent of a deceased court-record subject.

Those who argue against the purging of any arrest records often stress the fact that the arrestee can actually reassure prospective employers by showing a no-conviction disposition. Besides the doubts about how "reassuring" *any* arrest record, even one not resulting in a conviction, might be,[46] the fact remains that over one-third of the arrests

---

44. *Id.* at 495. Courts have generally shown a tendency to shield the media from liability for disclosing matters which are colorably of public interest even on nonconstitutional grounds. *See, e.g.*, Sidis v. F-R Publishing Corp., 113 F.2d 806 (2d Cir. 1940) (adult life of recluse who had been a celebrated child prodigy); Meetze v. Associated Press, 230 S.C. 330, 95 S.E.2d 606 (1956) (birth by twelve-year-old mother).

45. *See, e.g.*, Atchison, T. & S.F. Ry. v. Lopez, 216 Kan. 108, 531 P.2d 455 (1975) (privately maintained arrest records subpoenable but use restricted to equal employment hearing). *See generally* Appendix § 4(5).

46. For an excellent discussion of the impact of arrest records on job applicants' opportunities for employment, see Comment, *Discriminatory Hiring Practices Due To Arrest Records—Private Remedies*, 17 VILL. L. REV. 110 (1971). One survey reported that seventy-five percent of the New York employment agencies in its sample would not refer an applicant with an arrest record regardless of the disposition of his case. *Id.* at 127 n.144; *cf.* Gregory v. Litton Sys., Inc., 316 F. Supp. 401 (C.D. Cal. 1970), *modified on other grounds*, 472 F.2d 631 (9th Cir. 1972) (job application forms which asked about the applicant's arrest records held to violate Title VII of the Civil Rights Act, 42 U.S.C. § 2000e *et seq.*, since blacks were proportionately more likely to have been arrested). *See also* Morrow v. District of Columbia, 417 F.2d 728, 741-43 (D.C. Cir. 1969); Note, *Rehabilitation, Privacy and Freedom of the Press—Striking a New Balance*, 5 LOYOLA (L.A.) L. REV. 544, 563-67 (1972). One Federal Bureau of Investigation report indicates that only four percent of those arrested are held for prosecution. *See* Comment, 17 VILL. L. REV., *supra*, at 110 n.2. For a discussion of cases holding that an acquittal or a successful action for false imprisonment negates any subsequent prejudice from an arrest record, see Annot., 46 A.L.R.3d 900, 904 (1972).

reported to the National Crime Information Center (NCIC) are never followed by reports of disposition.[47]

Another more fundamental problem involves the retention of arrest records that have no disposition or show an acquittal. On the one hand is the argument that, justifiably or not, the person *was* arrested and historical facts should not be purged or erased; one cannot "unring the bell."[48] Police retention of such data is supported on the grounds that legal "technicalities" not reflective of the defendant's innocence of the charged violation have led to the decision not to prosecute or to an acquittal. There is also a reliance on statistical probability of guilt that is often based on a logical fallacy.[49] The erasure of such records can be supported on a variety of grounds ranging from common law privacy theories[50] to constitutional liberties.[51] Even when circumstances might

47. *See* PRESIDENT'S COMM'N ON LAW ENFORCEMENT & THE ADMINISTRATION OF JUSTICE, TASK FORCE REPORT: SCIENCE AND TECHNOLOGY 76 (1967) [hereinafter cited as TASK FORCE REPORT].

48. This anomaly leads to a related problem concerning job applications. If the statutory expunction model is followed, *see, e.g.*, ORE. REV. STAT. § 137.225(1) (1974), the subject of the record need not answer affirmatively to any question about such a no-disposition arrest. If the purging statute does not cover such a situation and the job applicant decides not to mention it, would a subsequent discharge caused by the employer's learning of the nondisclosure be justifiable? Similarly, if the arrestee were to bring a defamation action against a person who disclosed his arrest, should "truth" be a defense and, if so, how could it be proven?

49. *See* Morrow v. District of Columbia, 417 F.2d 728, 748 (D.C. Cir. 1969). The syllogism that a person who commits one criminal act is more likely than a previously law-abiding person to commit further crimes is no stronger than its minor premise—if the initial arrest was of an *innocent* person, the reasoning becomes fallacious. "The mere fact that a man has been arrested has very little, if any, probative value in showing that he has engaged in any misconduct. An arrest shows nothing more than that someone probably suspected the person apprehended of an offense. When formal charges are not filed . . . whatever probative force the arrest may have had is normally dissipated." Schware v. Board of Bar Examiners, 353 U.S. 232, 241 (1957) (footnote omitted).

50. In Eddy v. Moore, 5 Wash. App. 334, 487 P.2d 211 (1972), plaintiff was acquitted and successfully sought return from the police of the arrest records, fingerprints and photographs. The court said:

> Where the only reason for the presence of an individual's fingerprints and photographs in the police file is based upon an arrest which has subsequently been voided by an acquittal and no further justification is made for the retention of these fingerprints and photographs, no rational basis for their retention remains.
>
> . . . .
>
> . . . We have now reached the point where our experience with the requirements of a free society demands the existence of a right of privacy in the fingerprints and photographs of an accused who has been acquitted, to be at least placed in the balance, against the claim of the state for a need for their retention.
>
> 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

justify retention of such data[52] there seem to be no persuasive reasons to allow its dissemination to other than law enforcement agencies.

---

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, 85 S. Ct. 1678, 14 L. Ed. 2d 510 (1965).

Id. at 217.

51. In Menard v. Mitchell, 430 F.2d 486 (D.C. Cir. 1970), plaintiff sued to compel the removal of his fingerprints from FBI files. He alleged he had been arrested without probable cause, detained for two days and then released when California police were satisfied that no basis existed for charging him with a crime. The court, in the course of this opinion, made the following remarks:

> 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. 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.

Id. at 490-91 (footnote omitted). The court further stated:

> Many individuals have unjustly acquired arrest records without even the excuse of an honest and unavoidable mistake by the police. In the District of Columbia alone, literally thousands of persons were once arrested "for investigation" and then released; but their records often remain. Dragnet arrests are at best matters of recent memory. Even worse are those occasions, far more common than we would like to think, where invocation of the criminal process is used . . . often with no hope of ultimate conviction—as punitive sanction. Hippies and civil rights workers have been harrassed and literally driven from their homes by repeated and unlawful arrests, often made under sanction. Hippies and civil rights workers have been harassed and literally in mass arrests made to clear the streets either during a riot or during lawful political demonstrations. Use of the power to arrest in order to inflict summary punishment is, of course, unconstitutional; but even if the arrest was made lawfully and with the best of intentions, if the person arrested has been exonerated it is difficult to see why he should be subject to continuing punishment by adverse use of his "criminal" record.

Id. at 493-94 (footnote omitted).

In Menard v. Saxbe, 498 F.2d 1017 (D.C. Cir. 1974), the court held that the FBI Records Division must expunge criminal records if the reporting law enforcement agency advises that they are inaccurate. Similarly, it said that records must be expunged if the FBI has reason to know there was no probable cause for the arrest or that the arrest was unconstitutional. *But see* Voelker v. Tyndall, 226 Ind. 43, 75 N.E.2d 548 (1947). *See also* Kowall v. United States, 53 F.R.D. 211 (W.D. Mich. 1971) (acquittal); Hughes v. Rizzo, 282 F. Supp. 881 (E.D. Pa. 1968) (illegal mass arrest).

52. *See* 28 C.F.R. § 50.12(b) (1974) (FBI will not furnish arrest data more than one year old without indication of disposition); Appendix § 8(6). Oregon's abortive new legislation (see note 140 *infra*) had a provision for sealing records, but the file subject was required to convince the court that his or her "interest in privacy and reputation outweighs the public interest in maintenance of the record." As an additional precaution, all criminal record information distributed by a criminal justice agency was required to contain this notice: "All persons are advised that the information contained in this report can only be considered accurate for a period of six months from the date of this report. After such time this report should be considered inaccurate and should not

DOCTRINAL CONSIDERATIONS

The common law of torts has never completely defined the bounds of the invasion of privacy remedy. Because almost all cases reported in appellate opinions are instances of intentional behavior, we have little guidance with regard to negligent or innocent dissemination.[53] Similarly, if the data disseminated is not "intimate" information, the disclosure of which would shock the sensibilities of an ordinary person, the remedy might not apply. The reasons that personal compilations "leak" from credit bureaus and law enforcement agencies range from bribed or spiteful employees to employees who are recklessly indifferent to the fact that the data refers to a human being. Additionally, there are those who normally are conscientious but have a careless moment in failing to secure the data system or in failing to verify the identity and need to know of a data recipient.

If one assumes that a prudent actor could have avoided disseminating the data, it becomes important to consider whether data custodians owe a duty to file subjects. By virtue of the fact that they have a measure of control over the data system, the agencies or companies would seem to have such a duty.[54] Similarly, employees and agents who initiate action to process the data in such a way that it falls into the hands of a person without a recognized need to know should have a duty arising out of misfeasance.

There remains the nagging question whether the negligent breach of duty suggested above really causes the type of injury that a finder of fact can redress with a monetary award. If the recipient was not a person about to offer employment, settle or litigate a personal injury lawsuit, extend credit, underwrite insurance, or confer a security clearance and if the data was not intimate, economic injuries may not exist; and dignitary injuries may be so ephemeral as to deserve only a nominal award.

Two related phenomena suggest a countervailing policy, however. There has been some tendency, especially in government agencies, to merchandise salient portions of personal compilations in list form to commercial enterprises. To the extent that providing the information

be relied upon for any purpose." Law of July 8, 1975, ch. 786, § 4a, [1975] Ore. Laws — (repealed 1975).

53. Even modern privacy legislation only confers the civil damage remedy or imposes the criminal sanction in the event of "knowing," "intentional" and "willful" violations of the law. *See, e.g.*, 5 U.S.C.A. §§ 552a(g)(4), (i) (Supp. 1976).

54. *See* Tarlton v. Saxbe, 507 F.2d 1116, 1122-26 (D.C. Cir. 1974).

initially is either coerced by law (*e.g.*, business relationships in tax returns and security registration statements) or is required to obtain a governmental license (*e.g.*, applying for a private pilot's license),[55] or is derived from a particular purpose disclosure without warning of broader use (*e.g.*, requesting free information concerning hearing problems and ending up on a hearing aid manufacturer's mailing list), this practice debases an individual's sense of self identity and choice of relationships. Secondly, there is need to deter the general tendency of large institutions, whether governmental or private, to act oppressively or inhibitingly toward individuals who realize they are "en dossier."[56] Often the realization is incomplete, but its very incompleteness may produce anxiety, inhibition and other psychic crippling if the location, extent, and accuracy of the compiled data cannot be learned. Those most vulnerable to such anxieties, those most in need of "a fresh start in the colonies," may be those whose dossiers would detail past failures or embarrassments. But even the most successful among us should be nervous over the potential of unnecessary broadcasting of the details of our lives.

A certain amount of digitation is desirable and innevitable as automated data processing contributes sorely needed efficiency to the complex information needs of our society. Reasonable people may well differ as to the seriousness of the threat posed to our self identity by appearing on a mailing list. But if the familiarity of constant association with quantized data can lead to contemptuous indifference toward the individuals the data describes, strong deterrents to data misuse must be provided.

STATUTORY REMEDIES

In the context of institutional data custodians, it seems desirable to proscribe certain disseminations and to define a priori safeguards in

55. *See* A. MILLER, *supra* note 22, at 98.

56. *See* NAACP v. Alabama, 357 U.S. 449, 462-63 (1958); United States v. Rumely, 345 U.S. 41, 57-58 (1953) (concurring opinion); *cf.* Talley v. California, 362 U.S. 60, 64-65 (1960). In Menard v. Mitchell, 328 F. Supp. 718 (D.D.C. 1971), the court said:

> Systematic recordation and dissemination of information about individual citizens is a form of surveillance and control which may easily inhibit freedom to speak, to work, and to move . . . . 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.

Id. at 726. Some constraints on transfers of data between federal agencies are provided in 44 U.S.C. § 3508 (1970) (nonconfidentiality, consent, independent power to collect).

addition to allowing a tort remedy for those victimized. To this end, statutes and supporting regulations are the best vehicle. The Fair Credit Reporting Act is a notable effort in this direction.[57] The bill had a dramatic and turbulent evolution in Congress, but the legislation that emerged created some significant limitations on credit bureau behavior.[58]

The utility of the Act to curb abuses may be somewhat illusory, however, since there is a gap in the notification procedure. It is true that individuals are to be notified when a credit investigation of them is requested and are informed that they can request and receive a summary of the credit report generated by the investigation.[59] However, at the time of requesting credit the subject is often not concerned about the current report or, alternatively, fears jeopardizing the transaction pending by requesting the report.[60] If an individual either persuades the credit bureau of an inaccuracy or wishes to file unilaterally a dissenting declaration, he or she is entitled to notification of the fact that the bureau will send, on request, amended reports to recent recipients.[61] Because the individual's rights under the Act are not known to the average person, these notification provisions are obviously crucial to its efficacy as a curb to credit bureau inaccuracies and abuses. The most recent credit experiences of the individual may be remembered by him or her as innocuous enough; yet damaging and inaccurate material can be found in either investigative reports or one-sided reports of recent transactions. The only way for an individual to benefit from the statutory rights with regard to correction and updating of credit data is, of course, to see the file. But the right of access to the file is not required to be explained or mentioned in the first or second notices. Due to the absence of this crucial intermediate link, all but the most prejudiced or the most suspicious and determined individuals (or those who can afford to consult an attorney) will fail even to learn of the erroneous

57. 15 U.S.C. §§ 1681-1681t (1970).

58. *See* A. MILLER, *supra* note 22, at 86-88.

59. 15 U.S.C. § 1681d (1970).

60. It is true that whenever a detrimental decision with regard to insurance, credit or employment is based in whole or in part on a consumer report, the file subject is to be notified by the report user of the name and address of the reporting agency. *Id.* § 1681m(a). As to such detrimental decisions in the credit area alone and when they are based on reports *not* compiled by consumer reporting agencies, notification of the right to request disclosure of the reasons for the decision is required. *Id.* § 1681m(b). However subsection (b) would not apply to the typical case and even then falls short of the most meaningful notification.

61. *Id.* §§ 1681g-i.

material if it exists. Since the third notification (concerning the update rights) is only sent *after* a correction has been demanded[62] and few would seek a correction until after they had seen the entire file, this could turn out to be an empty gesture. The notification is important for those who reach the point of seeing an error in their file and should be preserved. However, to achieve the intended objectives, the notification gap must be corrected.

The Act provides civil redress for individuals who suffer actual loss due to negligent noncompliance with the Act.[63] There is also provision for punitive damages when the defendant acted in knowing noncompliance.[64] Credit information pertaining to transactions more than specified numbers of years in the past must be omitted from reports in all but exceptional cases.[65] Only specified entities may receive credit reports and investigative reports.[66] Procedures are to be employed by the bureaus to increase the accuracy of the data maintained and disseminated.[67] Whether the drafting loopholes and the timidity of file subjects reduce the Act to the political gesture category as its critics imply[68] or whether there is a de minimus number of abuses as the industry suggests[69] remains to be seen. Whatever the reason, there have been few appellate decisions since enactment of the Act despite a substantial

---

62. *Id.* § 1681i(d).

63. *Id.* § 1681o. *But see id.* § 1681h(e), which raises questions regarding a consumer's ability to maintain a defamation or negligence action against a reporting agency on the basis of information discovered through file access. There apparently has been no judicial interpretation of the scope of section 1681h(e).

64. *Id.* § 1681n(2). For a decision awarding $25,000 in punitive damages for FCRA violations see Millstone v. O'Hanlon Reports, Inc., 383 F. Supp. 269 (E.D. Mo. 1974).

65. For bankruptcies the period is fourteen years before the report date; for judgments, seven years or the statute of limitations, whichever is longer; for criminal records, seven years. These chronological cutoffs do not apply to credit transactions or life insurance involving $50,000 or more or employment at an annual salary of $20,000 or more. 15 U.S.C. § 1681c (1970).

66. See note 26 *supra.*

67. 15 U.S.C. § 1681e (1970). The statute requires the agencies to "maintain" and "follow reasonable procedures" to insure compliance with disclosure limitations and file accuracy. In the area of disputes with a file subject over accuracy, the agency may decline to make changes or additions if it has "reasonable grounds to believe that the dispute by the consumer is frivolous or irrelevant." Similary, it can refuse to transmit the consumer's statement of dispute. *Id.* § 1681i. However, harassment of agencies by crank complaints is felt to be negligible. In fact, nearly all of the subject access interviews do lead to some modifications of the file but these are predominantly updates and improvements rather than disputes. Telephone interview with Barry Connelly, *supra* note 19. These additions are in the best interests of all parties concerned.

68. *See, e.g.*, A. MILLER, *supra* note 22, at 88.

69. *See Hearings on H.R. 16340 Before the Subcomm. on Consumer Affairs of the House Comm. on Banking and Currency*, 91st Cong., 2d Sess. 122, 458-505 (1970).

number of file subject accesses.[70] An alternative explanation could be that there are abuses, but, that since the most common injuries (inconvenience and temporary embarrassment) are not worth much in compensation, few persons sustain enough "actual losses" to make suit worthwhile. If this is the correct explanation, it is doubtful that the threat of a rare lawsuit will be sufficient to alter bureau procedures. The Act could, nevertheless, have a desirable impact if coupled with media publicity and employee training programs.

In the criminal justice area, Iowa was the first state to enact a tough record-privacy statute,[71] and bills concerning criminal record privacy were introduced in several state legislatures in 1975.[72]

A substantially amended version of Senator Sam Ervin's privacy bill was enacted on the last day of the Ninety-Third Congress.[73] This legislation employs an omnibus approach and covers virtually all records pertaining to and identifiable by reference to individuals and maintained, used, collected, or disseminated by virtually all federal agencies.[74] Transmission of such data from a non-law enforcement agency to an authorized law enforcement agency can only be accomplished if a written request is received from the agency head.[75] File subjects are granted access to their records and an opportunity to request corrections or additions and file a statement of disagreement if such a request is refused.[76] Agencies are required to deal, insofar as is practicable,

70. In 1972 members of the Associated Credit Bureaus reported 1,713,000 file disclosures. They estimate there were approximately two million disclosures (on a base of 100 million credit reports) in 1974. Of the 1972 disclosures, 1,304,000 or around seventy-five percent were triggered by a notice of denial of credit. The average cost to the agency of such disclosure interview is thought to be between $2.60 and $3.00. There were 74,000 consumer statements entered in 1972 by ACB members indicating that bona fide unresolvable disputes arose in about 4½% of the cases where disclosures were made. Telephone interview with Barry Connelly, *supra* note 19.

71. IOWA CODE ANN. § 749B (Cum. Supp. 1976). For an outline of the suggested contents of a privacy statute see Comment, *Privacy, Law Enforcement, and Public Interest: Computerized Criminal Records*, 36 MONT. L. REV. 60 (1975).

72. *See, e.g.*, [1975-1976] Cal. Gen. Sess., chs. 883 (no public agency can require disclosure by an applicant for registration or license of arrests not leading to conviction or nolo contendere plea), 904 (allowing court to order sealing of arrest record followed by acquittal based on "factual" innocence), 1043 (prohibiting employers from asking questions about arrests not leading to convictions or not pending trial disposition at any stage of employment or employment application). *See also* CAL. PENAL CODE § 11124 (Supp. 1975) (conferring right of criminal history file subject review).

73. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, § 3 (codified at 5 U.S.C.A. § 552a (Supp. 1976)).

74. The definition of a federal agency is found at 5 U.S.C. § 551(*l*) (1970) and 5 U.S.C.A. § 552(e) (Supp. 1976) (added in 1974 over a presidential veto).

75. 5 U.S.C.A. § 552a(b)(7) (Supp. 1976).

76. *Id.* § 552a(d).

directly with the file subject whenever the information needed could result in "adverse determinations about an individual's rights, benefits and privileges under Federal programs."[77] Notice is required to inform the public of the procedures to be utilized for any individual to determine whether an agency has a file pertaining to him or her.[78]

Civil remedies include federal judicial review of agency refusals to correct or to grant access and actual damages in cases of "intentional or willful" inaccuracies or violations of disclosure restraints.[79] Intentional violations of disclosure and notice requirements are misdemeanors subject to fines of up to 5,000 dollars.[80] Political surveillance material may not be maintained although law enforcement agencies are exempted from that prohibition as long as the data is "pertinent to" and "within the scope of" the agency's activity.[81]

Notwithstanding the salutory objectives and comprehensive approach to the Act, law enforcement agencies are permitted to institute rulemaking proceedings for the purpose of exempting their record systems from certain of its provisions.[82] Among the avoidable provisions are the subject's right of access to the file, the subject's right to know *if* a file is being maintained on him or her, and the ability to learn who has accessed the file.[83] The extent to which law enforcement agencies will succeed in exempting their record systems is as yet undetermined.

State agencies that handle criminal history information the processing of which is funded in whole or in part by Law Enforcement Assistance Administration (LEAA) funds are subject to federal regulation. Recently promulgated LEAA regulations suggest that states maintain a central repository, and require that a record of the disposition of an arrest be sent to the repository within the seemingly lengthy period of ninety days following such disposition.[84] The burden is on

77. *Id.* § 552a(e)(2).
78. *Id.* § 552a(e)(4)(G).
79. *Id.* § 552a(g)(4). There is a minimum civil recovery of $1,000.00. *Id.*
80. *Id.* § 552a(i).
81. *Id.* § 552a(e)(7).
82. *Id.* §§ 552a(j)-(k). The reasons for any exemptions must be annually reported to Congress by the President. *Id.* § 552a(p).
83. *Id.* §§ 552a(j)-(k). Understandably, law enforcement agencies will want to exempt subject access from investigatory or intelligence data. Even here, however, the agency must disclose such data to the subject if he or she is "denied any right, privilege or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material." *Id.* § 552a(k)(2). Other types of record systems which may be exempted include secret service investigations, federal employment investigations and test results, and armed forces promotion evaluation data. *Id.* §§ 552a(k)(3), (5)-(7).
84. 28 C.F.R. § 20.21(a)(1) (1975). *See also* the amendments to these regulations in 41 FED. REG. 11714-18 (1976).

disseminating agencies to query the state repository before local dissemination, and originating and repository agencies must notify all criminal justice agencies known to have previously received the relevant data of any errors subsequently discovered.[85] Direct or indirect employee requests for verification of the non-existence of a criminal record are forbidden.[86] These audits are to be done in a "representative sample of State and local . . . agencies chosen on a random basis."[87] The length (chronologically speaking) of the audit trail is not specified, although a paragraph requiring that the file subject be given, on request after a record correction, the names of all non-criminal justice agencies accessing challenged data could be read to suggest an openended period.[88] Private entities may access non-conviction records if they are "authorized by statute, ordinance, executive order, or a court rule . . . as construed by appropriate date or local official or agency."[89] Since state law enforcement agencies, especially those which are endeavoring to automate their criminal history files, are frequently heavily dependent on LEAA funds, these regulations should have a substantial and early impact.

As in credit reporting, the ideal statute allows the obviously necessary practices of data gathering and recordkeeping to continue, but places constraints on access and dissemination, allows some measure of subject access and corrective or explanatory input, and provides civil remedies for noncompliance. The nationwide shift toward automated information systems not only increases the complexity of the problem but also suggests that negligence-proof procedures can be developed and better monitoring can be achieved.[90] Budget-conscious law enforcement agencies can be expected to raise cost-benefit objections to such legislation. The cost of software and storage to implement safeguards can be quantified and concededly is not negligible.[91] In contrast, injury to the file subject and the indirect injury to society from confidentiality abuses are very difficult to quantify. Moreover, there is the implied

85. *Id.* §§ 20.21(a)(1)-(2). The obligation of prior verification is suspended in cases where "time is of the essence and the repository is technically incapable of responding within the necessary time period." *Id.*

86. *Id.* §§ 20.3(k), 20.21(b) & (c), *as amended*, 41 FED. REG. 11715 (1976). The limits do not apply to conviction data. *Id.* For one state's attempt to legislate similar limits see note 140 *infra.*

87. *Id.* § 20.21(e), *as amended*, 41 FED. REG. 11716 (1976).

88. *See id.*

89. *Id.* § 20.21(g)(4).

90. *See* A. WESTIN & M. BAKER, *supra* note 19, at 268.

91. *See generally* L. HOFFMAN, SECURITY AND PRIVACY IN COMPUTER SYSTEMS (1973).

argument that privacy safeguards are implemented at the expense of efficient law enforcement.

Even among those who agree that some statutory safeguards must be provided, there are differing approaches. Politicians and law enforcement professionals often favor a brief policy-oriented statute delegating authority to promulgate implementing regulations to law enforcement agencies. A statutory privacy commission might be a satisfactory alternative.[92] If no such commission is created, the most logical agency to draft and enforce the regulations is usually the state police. With regard to personnel screening, training programs and physical and electronic security, the problems are best handled by the agency that manages the system.[93] However, on broader issues such as rights of file subjects, standards for audit of performance, need to know, and constraints on dissemination, the regulation model seems less satisfactory. Even if one assumes that typical administrative procedure act public hearings are held before the proposed regulations become final, the theme and main outlines of the safeguard program will be almost irrevocably set in advance. Understandably, the drafters will choose to regulate in a manner which will minimize costs, difficulties, and embarrassments; indeed, to do otherwise would probably be contrary to their overall management objectives. But this commendable sense of internal efficiency makes them ill suited to draft regulations dealing with a problem that has important external as well as internal ramifications.

92. The Privacy Act of 1974 creates a Privacy Protection Study Commission of seven appointed persons chosen for their expertise in the areas of civil rights, law, computer technology and records management among others. In addition to its investigatory, analysis, assistance and recommendatory powers, the Commission can, "upon request, prepare model legislation for use by State and local governments." Act of Dec. 31, 1974, Pub. L. No. 93-579, §§ 5(b)-(d), 88 Stat. 1896.

The MODEL STATE ACT FOR CRIMINAL OFFENDER RECORD INFORMATION, drafted by the staff of System for Electronic Analysis and Retrieval of Criminal Histories (funded by participating states and LEAA), contained provisions for a Criminal Offender Records Control Committee, *id.* § 4 (law enforcement officials to promulgate regulations), and for a Security and Privacy Council, *id.* § 5 (nine members including some from outside the criminal justice community). Recent legislation in Oregon provided for a Criminal Record Council of nine appointed persons to advise the Governor and approve of rules adopted by him to implement criminal record privacy and security requirements, as well as record verification and operational audits. Law of July 8, 1975, ch. 786, §§ 7-7b, [1975] Ore. Laws —. The legislation was subsequently repealed, however, due to an inadvertant defect. Law of Sept. 16, 1975, ch. 1, [1975 Special Session] Ore. Laws —. See note 140 *infra* for a discussion of the difficulties that befell the Oregon act.

93. *See* Appendix § 11(1). However, even the relatively exemplary New York State Identification and Intelligence System was found by state auditors to have failed to control access by federal employees, to institute a formal employee training program, and to utilize security clearance for internal access. A. WESTIN & M. BAKER, *supra* note 19, at 312-13.

Moreover, public input tends to be largely responsive rather than creative. Criticism runs to suggestions for a better phrase here and the deletion of a word there, or to emotional objections that the whole scheme is unacceptable. Seldom are any substantial alternatives proposed to displace or modify the general thrust or tenor of the proposed rules. The trade-offs and overall policies decided upon by the drafters usually emerge unchanged.

For this reason it seems extremely desirable that the social policies, the economic sacrifices, and the procedural balance points be definitively determined by the elected representatives of the people, however difficult and politically nerve-racking that may be. The interdependencies are fairly complex; a certain amount of technological understanding is required; and not all political constituencies can be satisfied. Thus legislators must work hard and make politically sensitive trade-offs. Still, this *is* the legislature's function, and the competing public interests make it the most appropriate body to grapple with the problems and resolve the tensions. A model statute has been drafted by the author and reprinted in the Appendix to this article.

Proposed Statutory Solution

It is by no means straightforward to define the types of criminal records systems to be covered by a statute. Computerized systems are capable of instantaneously interfacing with remote terminals and thus present aggravated problems in verifying the accessor's identity and need to know. On the other hand, systematic and automatic procedures for verification and updating of data are available in computerized systems. Finally, the technological aspects of systems using dedicated computer storage, remote online terminals, hard copy printers, and common carrier communications networks are sufficiently complex that accurate and discriminating definitions must be employed.[94]

Equally difficult is the task of defining what data shall come within the purview of the statute. In addition to careful, inclusive use of terminology, conceptual problems arise. Are traffic violations to be lumped with felonies and other misdemeanors? Are juvenile custodial reports to be treated like arrests? Are pre-sentence investigation reports objective or subjective? What if law enforcement personnel assist in the search for a missing person? Should the use of intelligence data be constrained?[95] The approach taken in the draft statute was to focus on

94. *See* Appendix §§ 1(2) (information system); 1(12) (purge); 1(13) (seal).

95. See *id.* §§ 4(3)(h) (disclosure of traffic convictions); 8(2) (forfeiture of bail in traffic citations); 1(4), 8(7) (juvenile custody reports and sealed records); 1(3)

"compilations,"—data that is organized around or can be retrieved by or manipulated through an individual's identity referent.[96] Since the greatest threats to privacy arise when criminal justice data is collated and aggregated to focus on particular individuals, constraining the use of compilations should produce the greatest protection at the least cost.

A further problem in any comprehensive statutory approach is to define subsets of criminal justice information. Access criteria will vary with functional purpose and content sensitivity.[97] Correctional information, for example, may include both subjective and objective data. It may be appropriate to disclose some portions while disclosure of other portions would unquestionably be detrimental to the rehabilitative process.[98]

Constraints on access will be ineffective if the definitions of users and types of inputs and readouts are lacking in precision and clarity.[99] For example, the draft act definition of "disposition" presented difficulties due to the wide variety of post-arrest events that should be recorded.[100] Since the statute would require erasure of references to dispositions reflecting innocence,[101] the problem was further complicated.

The draft statute attempts to curtail abuses of the possession of the compiled data *inside* the criminal justice agencies by requiring a need to know for initial access and hard copy production.[102] Although such standards can be articulated, there is reason to believe that employee indifference and competing job priorities will cause such standards to be often disregarded. If this is so, the incremental gains of such safeguards may not equal their incremental costs.

As systems become networked and linked to criminal justice agencies in other states, the problem of enforcing safeguards becomes acute.

(pre-sentence investigation reports); 6 (missing persons); 1(9) (intelligence data); 12 (intelligence data).

96. *See id.* § 1(1).

97. *Compare id.* §§ 1(3), 5(1)(b) (access for research) *with id.* § 4(3) (potential employers) *and id.* § 3(1) (out-of-state law enforcement agencies).

98. *See, e.g.*, Turner v. Reed, 538 P.2d 373 (Ore. App. 1975) (psychiatric examination reports and information concerning family life of prison inmate exempt from disclosure but purely factual data used by parole board not exempt).

99. *E.g.*, Appendix §§ 1(14) (criminal justice agency); 1(11) (dissemination); 1(15) (hard copy); 1(17), 9(3)-(6) (audit entry).

100. *See id.* § 1(10). *See also* Alexander & Walz, *Arrest Record Expungement in California*, 9 U.S.F.L. REV. 299, 302 n.15 (1974), *quoting* CAL. PEN. CODE § 11116 (West 1970).

101. See Appendix § 8(2).

102. See *id.* § 2(1).

Apart from questions of extraterritorial power and federalism,[103] severe difficulties arise in preventing access by agencies not under similar constraints. The networks can operate automatically, *i.e.* without human intervention, and instantaneously (assuming the retrieval computer is "on line"). The model statute attempts to solve this issue by the use of standing interagency covenants (treaties) providing that the requesting agency is aware of and will comply with the constraints applicable to access and dissemination in the repository agency's state.[104]

The question whether employers should be able to access or receive criminal justice information concerning employees and job applicants is evenly balanced. It must be conceded that a great many people believe that, all other things being equal, the applicant with a conviction record should not get the job over an applicant who has no nontraffic convictions. Unlike racial or sexual discrimination, it can be argued that such discrimination is not based on mere suspicion or unfounded notions of inferiority, but rather is predicated upon a historical demonstration of anti-social behavior. Whether this distinction would be broad enough to survive a job-related requirements test in state or federal regulations designed to protect ex-convicts remains to be seen.[105] The widely held belief that an employer has an inalienable right to hire whom he pleases and that in order to exercise that right he is entitled to check applicants' criminal records also seems dubious. Such diverse constraints as union shops (reached via collective bargaining agreements) and minority hiring quotas (required under government procurement contracts) would seem to have already eroded this employer prerogative[106] which, in any event, is not a fundamental freedom of federal constitutional stature.[107]

The statute strives for a compromise by allowing selective release of *some* criminal justice information to *some* employers when a functional nexus is evident.[108] There is an attempt to control secondary use and

103. *See* text accompanying note 37 *supra.*

104. *See* Appendix §§ 3(1)-(2).

105. *Cf.* Griggs v. Duke Power Co., 401 U.S. 424 (1971) (Civil Rights Act of 1964 and racially selective employment tests).

106. The employer could claim that contractual agreements are consensual and not external constraints. However, sometimes its bargaining power may be so weak that it has little alternative except to liquidate its business.

107. In the absence of legislation compelling a contrary result, such employment discrimination could continue in cases in which state action could not be proven. However, if and when the legislature saw fit to proscribe such employment practices, the employer's "right" would be terminated absent a showing of a job-relatedness.

108. *See* Appendix § 4(3).

dissemination by placing restraints on the recipients (employers) of this information.[109] Violation of these restraints can give rise to criminal prosecutions.[110]

Access for court administration and sociological research purposes is allowed by the draft act. Some research access proposals allow access only when the result is to be collectivized, statistical findings. Case history longitudinal studies may need to focus on selected individuals, however, and this type of research can be highly useful in corrections work. In any event, nondisclosure agreements or similar safeguards against the public dissemination of the actual identities of living file subjects should be insisted upon.[111]

In addition to disclosures for law enforcement and employment purposes, there are often other justifiable reasons for disclosing criminal justice information. The statute would allow probation and parole officers to represent orally the substance of file information to assist in the social, economic and educational rehabilitation of criminals.[112] Judges are allowed to reveal such selected criminal justice information through comments in open court and published opinions and orders as, in their discretion, is appropriate for the overall purposes of the criminal law.[113]

In the controversial area of arrest records,[114] the model statute requires purging of records of arrests only when no disposition is shown, charges have been dropped, probable cause was not found, there has been a decision not to prosecute, or there has been an acquittal on the merits.[115] A record of an arrest followed by an acquittal based on insanity or a pardon must be retained, as must a record followed by a

109. *See id.* § 4(4).

110. *See id.* § 13(5).

111. See *id.* §§ 5(4)-(6). *See* State *ex rel.* Carroll v. Junker, 79 Wash. 2d 12, 482 P.2d 775 (1971) (researchers denied access to files of individual randomly selected mental institution inmates despite offer of confidentiality).

112. Appendix § 7(1). The consent of the file subject is required. This feature may draw the objection that only positive material would be released. However it should be remembered that if the criminal justice information were job-related, it would be accessible to an employer in any event. *See* text accompanying note 108 *supra.* Moreover, a parole officer is not precluded from giving a general opinion (as contrasted to specific record information) about the character, stability and rehabilitative prospects of a person under his jurisdiction even without the consent of such person.

113. *Id.* § 7(2). This is similar to the absolute immunity enjoyed by judges under defamation law, but is phrased to encourage greater sensitivity and discretion on the part of the judiciary.

114. *See* text accompanying notes 48-52 *supra.*

115. Appendix § 8(2).

conviction, guilty plea or nolo contendere plea,[116] since all of these dispositions are consistent with a justifiable (after the fact) arrest.

The difficulties of "tracking" arrest dispositions from law enforcement agencies to prosecutors' offices to courts to record custodians are manifest. The statute places the initial burden of updating arrest information with disposition data on the agency that originated the original entry. It additionally places an obligation on the information system to query the originating agency every ninety days until a permanent disposition is reflected. If eighteen months pass without a disposition and the arrestee has not been a fugitive during such period, the arrest record shall be purged in all but intelligence files.[117] It has been suggested that prosecution be barred if the trial is not commenced within some finite, relatively short time as an alternative to purging the arrest record.[118] Salutory as this limitation might be, it does not necessarily insure that the disposition will reach the compilation and be linked to the arrest record. Nor does it erase the potential stigma of having an arrest record even when there is also a record of a subsequent acquittal.[119]

There may be circumstances in which criminal justice officials feel strongly that records of arrests not followed by a disposition should not be purged. Provision is made in the draft act for the agency to administratively petition the governor to retain such records.[120] Unlike some public records legislation in which the burden of proof is on the entity seeking nondisclosure,[121] the burden under the proposed draft would be on the agency seeking retention.[122]

The proposed statute does not purport to address the broader questions of when and why conviction records or juvenile records should

116. *Id.* A pardon is sometimes unrelated to guilt (*e.g.*, when material exonerating evidence comes to light after trial) but is included as a basis for retaining the arrest record since other criminal justice records, *e.g.*, criminal court and corrections, inevitably will have been generated in such cases, the arrest will have been supported by probable cause, and the pardon does not invariably reflect complete innocence.

117. *Id.* §§ 8(2)-(5).

118. For an example of federal legislation passed primarily for other reasons, but incidentally having this effect, see Federal Speedy Trials Act, 18 U.S.C.A. § 3161 (Supp. 1976).

119. *See* notes 46-47 and accompanying text *supra.*

120. Appendix § 8(6).

121. *See, e.g.*, ORE. REV. STAT. §§ 192.500(2)(a), (d) (1973).

122. An admittedly difficult case would involve an acquittal based on a bill of rights issue where objective evidence indicated guilt. The bracketed language in section 8(6) of the draft statute is an attempt to cope with this situation, but it must be admitted that any such criteria are extremely difficult to formulate and may be politically unacceptable as well.

be sealed or expunged. It does, however, require a procedure to be followed by criminal justice record custodians should a court order or statute require sealing or purging.[123]

Seemingly implicit in conferring on a file subject the right to examine and suggest corrections to his or her compilation is the right to know to whom the compilation has been disseminated.[124] Only in this way can the subject be personally assured that past recipients of prejudicial errors have been notified of the inaccuracy. Even when errors are discovered through internal audit procedures, a log of who has received information from the file is necessary to send out corrections. Both manual and automated systems can maintain such logs, known in the jargon as "audit trails." Access to a compilation, whether stored in a computer or in manual files, can take several forms and have various purposes (*e.g.*, read-in, read-out, process). Thus, care must be used in defining when an audit entry is required and what, at a minimum, the entry must include.[125]

It is one thing to statutorily require audit entries for the production of hard copies or for manually accessed files, but it is quite another to enforce such a requirement. Training and education can help, and the deterrent effect of the criminal sanction may also play a role. Computerized systems can be programmed to deny access until an audit entry has been tendered, but no such leverage exists once the data is outside the computer files. The proposed legislation proceeds on the assumption that it is better to require audit trails than to leave the safeguards entirely to the day-to-day care and good faith of the system operators.[126]

The chronological length of the audit trail determines the completeness of the correction of erroneous data. Since longer trails take more space in computer storage, they also cost more. The economic factor is a trade-off that legislatures will have to make. The proposed statute employs a four-year period.[127] Cheap systems protect less thor-

123. Appendix § 8(7).

124. *See id.* § 10.

125. *See id.* §§ 9(3)-(6).

126. The draft statute calls for biennial auditing by the system operators with reports to the Governor of the findings and corrective actions taken. *Id.* § 11(5). Others have recommended that a separate agency should conduct the audit. See TASK FORCE REPORT, *supra* note 47, at 75.

127. Appendix § 9(1). The Privacy Act of 1974 calls for retention of the audit trail (therein called an "accounting") for five years or the life of the record, whichever is longer. 5 U.S.C.A. § 552a(c)(2) (Supp. 1976). Apart from the file-subject's remedies, an audit trail retention period of at least two years should be employed for internal training, disciplinary and reprimand procedures.

oughly; on the other hand, after a sufficient period elapses, it is safe to assume no future prejudice can befall the file subject and that past prejudice has become irremediable.[128]

There is broadly based support for allowing file subjects to examine compiled criminal justice records. The examination right does not extend to intelligence data.[129] While this distinction may seem hypocritical to a privacy purist, it is rationally supportable if any value is placed on pre-arrest surveillance and investigation as a weapon to reduce crime. To further justify this distinction, intelligence data should not be used for non-law enforcement purposes, and political or ideological dossiers unrelated to criminal acts should not be maintained.[130] A concommitant of the right to examine is the procedure for requesting corrections, clarifications, or additions to the compiled record. The model act requires that an explanation of this procedure be given the subject at the time of the examination.[131] If the request is denied in whole or in part, the file subject may take an administrative appeal under the state administrative procedure act.[132] The burden of justifying the change is placed on the file subject.[133]

Since these procedures all take time, the statute addresses the problem of contemporaneous dissemination with particularity. Entries are required to be made so that persons accessing the file will be aware that a review or challenge is pending.[134] If a permanent change is made at any administrative level, the system must inform agencies, entities and other information systems that have accessed the information in the past of the updated version.[135]

The proposed statute does not confer new civil causes of action on behalf of file subjects against people outside criminal justice agencies who access or disseminate data in violation of the statute. It does preserve whatever rights may exist by common law.[136] This approach

128. Law enforcement officials contend that no responsible entities work with or make decisions based upon stale criminal histories and that a much shorter period is sufficient to protect the file subject.

129. Appendix § 10(5). *See also* 5 U.S.C.A. §§ 552(b)(1)(A)-(B) (Supp. 1976).

130. See *id.* §§ 3(1)-(2), 12(2).

131. *Id.* § 10(4).

132. *Id.* §§ 10(7)-(8), (11)-(13).

133. *Id.* § 10(13).

134. *See id.* § 10(9).

135. *Id.* §§ 10(14)-(15). The "reachback" time is four years for criminal justice agency recipients and two years for other recipients. *Id.* Section 10(10) requires all information systems so notified to change their own records to comport with the updated version.

136. *Id.* § 13(4). For a discussion of common law causes of actions and remedies see Carr v. Watkins, 227 Md. 578, 177 A.2d 841 (1962) (false light privacy action).

has, to be sure, some disadvantages since "insiders" may be able to cover their tracks and the greatest damage may be done by "outsiders." An additional drawback may be that "insiders" are typically individuals of modest resources whereas "outsiders" may be sizable corporations.

Since the greatest merit in such a statute is its preventive impact rather than its remedial impact, it has focused primarily on criminal sanctions against all violators and on internal safeguards that can be readily monitored. As a supplementary measure, statutory civil recoveries of actual damages (or 1000 dollars, whichever is greater) are provided against "insiders."[137]

The concept of an independent "watch dog" criminal records privacy commission has enjoyed considerable currency.[138] The commissioners in such models are either wholly public members or are balanced between law enforcement members and non-law enforcement members. Such commissions could be authorized to promulgate regulations and safeguards to control the operation of criminal justice data systems. This approach has not been utilized in the proposed statute. The effort was to *avoid* the creation of an additional governmental body while still achieving the purpose of allowing the administrative resolution of disputes as to file accuracy, rights to access, and record retention with an opportunity for judicial review.

The author concedes that this proposal may not be politically viable, at least as a complete package. The political strengths in this area tend to be unusually polarized—the American Civil Liberties Union and others of strong and deeply felt concern about personal privacy on one side and the law enforcement professionals on the other. Both sides are in fact willing to make some compromises but the groups often adopt extremist strategies. Thus, a proposal which attempts to be "down the middle," treating each subissue on its independent merits, will not likely gain support from either side. Despite fairly extensive coverage in the press and in popular books,[139] there is little interest in criminal justice privacy among law-abiding middle class citizens who will not identify with the problem even though they could easily become involved as an employer or a victim of a mistaken identity arrest. Thus,

137. Appendix § 13(1). The Executive Director of the American Civil Liberties Union, Aryeh Neier, has urged that criminal sanctions be extended to cover "outsiders" as well as "insiders." *See Hearings on H.R. 13315 Before Subcomm. No. 4 of the House Comm. on the Judiciary*, 92d Cong., 2d Sess. 163 (1972).

138. *See, e.g.*, IOWA CODE ANN. § 749B.19 (Cum. Supp. 1976); Law of July 8, 1975, ch. 786, §§ 7-7b, [1975] Ore. Laws — (repealed 1975).

139. *E.g.*, A. MILLER, *supra* note 22.

those who are concerned and exert political pressure tend to support more extreme solutions while those who might perceive the problem and its solutions more objectively are seemingly not involved.[140]

OTHER AREAS OF ABUSE

Other possible contexts in which one can expect complaints of misuse of accurate information are commercial and political competition. A manufacturer might hire an investigator to uncover an embarrassing quality control error by the competition or to catalogue manufacturing liability lawsuits filed against a competitor. Assuming

140. The State of Oregon enacted criminal records privacy legislation in 1975 and the story of its development and subsequent repeal is worth noting. The Oregon Law Enforcement Council (OLEC) consists predominantly of legislators and law enforcement officials and is appointed by the Governor. The Council designated a task force of its members and a few *ex officio* members representing, *inter alia*, the ACLU, and an urban public defender office to draft a criminal record privacy bill for eventual presentation to the legislature. The drafting process took nearly nine months and the legislature was already in session when the eleventh draft from the task force was presented to a plenary meeting of the OLEC. The prevailing sentiment on the OLEC was diametrically opposed to limits on dissemination of arrest records. As a result, this aspect of the draft legislation was eviscerated.

The OLEC bill was strenuously attacked during hearings before the House Judiciary Committee. Consequently, the majority of the Committee passed out a bill (H.B. 2579) on April 21, 1975, which went considerably beyond the OLEC Task Force's eleventh draft in protecting privacy. This bill passed on the floor of the House on April 24 by a moderately wide margin despite support for the Committee minority's compromise version. During hearings before the Senate Judiciary Committee, LEAA regulations pertaining to criminal records systems receiving LEAA funding were promulgated. In an effort to tighten the coverage of the bill and, at the same time, to comply with LEAA regulations, the ACLU representative convinced the Committee in the closing days of the session to employ the LEAA definitions nearly verbatim. Through inadvertance, however, the correlative LEAA exemptions were not incorporated. Several days after the House vote, the omission was discovered, but rather than pull the bill back from the floor of the Senate, a separate bill (S.B. 716) was developed to cure the defect. Both bills eventually passed the Senate, on June 9 and 13, respectively, and were sent to the House. Lack of awareness of the significant interdependence of the two bills and last-minute parliamentary maneuverings on the floor of the House resulted in passage of the basic bill on June 10 although the corrective bill never was debated or put to a vote.

Just before the effective date, September 13, 1975, law enforcement officials realized the impact of the now overinclusive legislation. An Opinion of the Attorney General dated September 9 confirmed their interpretation that the news media were totally foreclosed from access to criminal justice records. This led to intense publicity by the news media with front page coverage on successive days stressing the first amendment implications and characterizing the act as police-state legislation. Final Legis. Calendar, Regular Sess. 1975, 58th Legis. Assembly of the State of Oregon, H-87 to -88. The Governor called a special session of the legislature and, although there was a half-hearted attempt to amend the bill to include the omitted exemptions and to clarify an ambiguity regarding next-of-kin notifications, the entire statute was repealed at a one-day session on September 16, 1975. Law of Sept. 16, 1975, ch. 1, [1975 Special Sess.] Ore. Laws —.

unflattering discoveries were made, he could then utilize the material in an advertising campaign. Similarly, such information could be used by lobbyists urging legislation designed to impede the competition. Proponents of ideological ballot measures or candidates for elective office could employ the same tactics.[141] Generally, the use of information in such ways is protected on first and fourteenth amendment principles[142] or under the right to petition the government.[143] But the so-called "commercial speech" exception could be applicable to deprive business competitors of constitutional immunity.[144] Even without specific immunity, however, there may be no liability if the use is not tortious under common law or statutes. The Federal Trade Commission usually does not attempt to enjoin invidious comparison advertising based on relevant facts,[145] and anything that delivers more information to the marketplace or the governmental decisionmaker is usually countenanced.[146]

On balance, the public's need to know would seem to suggest no recovery for such dissemination. This conclusion has particular force when qualified privileges (for competitors or those commenting on public officials and candidates) are available even to those who disseminate *mis*information under the law of defamation.[147]

---

141. *Cf.* Corman v. Blanchard, 211 Cal. App. 2d 126, 27 Cal. Rptr. 327 (2d Dist. 1963) (sustaining of demurrer against libel complaint affirmed). Certainly the disclosure of facts about Senator Eagleton's unfortunate medical history was appropriate at the time of considering the Senator for the Vice Presidential candidacy. *See generally* Note, *Invasion of Privacy—Disclosure of Contents of Wrongfully Obtained Documents of Public Figure*, 55 MINN. L. REV. 156 (1970).

142. *Cf.* New York Times Co. v. Sullivan, 376 U.S. 254 (1964) (libel of public official requires showing of recklessness or knowing falsity).

143. *See* Eastern R.R. Presidents Conference v. Noerr Motor Freight, Inc., 365 U.S. 127 (1961).

144. *Cf.* Pittsburgh Press Co. v. Pittsburgh Comm'n on Human Relations, 413 U.S. 376 (1973); Columbia Broadcasting System, Inc. v. Democratic National Comm., 412 U.S. 94 (1973); Valentine v. Christensen, 316 U.S. 52 (1942). *But cf.* Bigelow v. Virginia, 421 U.S. 809 (1975); Murdock v. Pennsylvania, 319 U.S. 105 (1943).

145. See *Developments in the Law—Competitive Torts*, 77 HARV. L. REV. 888, 897 (1964) for the inference that the Federal Trade Commission will not countenance comparisons based on misleading or irrelevant facts. The Federal Trade Commission Act, 15 U.S.C.A. § 45(a) (1973), does not confer private remedies. Smith-Victor Corp. v. Sylvania Electric Products, Inc., 242 F. Supp. 302 (N.D. Ill. 1965).

146. *See* FTC v. Sterling Drug, Inc., 317 F.2d 669 (2d Cir. 1963); *cf. In re* Cape Cod Broadcasting Co., 22 F.C.C.2d 403 (1970) (competitor for broadcast license compelled disclosure of licensee's financial reports submitted to FCC). *But cf. In re* Sioux Empire Broadcasting Co., 10 F.C.C.2d 132 (1967).

147. *See, e.g.*, New York Times Co. v. Sullivan, 376 U.S. 254 (1964) (public officials); Kemart Corp. v. Printing Arts Research Labs., Inc., 269 F.2d 375 (9th Cir.), *cert. denied*, 361 U.S. 893 (1959) (infringement claim); Coleman v. MacLennan, 78 Kan. 711, 98 P. 281 (1908) (candidate).

CONCLUSION

Tort law provides some protection for victims of unauthorized use of accurate information by means of the seldom invoked concepts of prima facie tort and by undue publicity in the invasion of privacy area. The latter concept is limited, not without some justification, to situations involving revelations of intimate facts to sizable numbers of people. With the increasing depersonalization of bureaucratic recordkeeping and the utilization of computerized data banks, it may be that additional tort remedies will have to be created by statute. Alternatively, courts must be ready to hold that data compilers and custodians owe a duty to the subjects identifiable in the data.[148] Questions of breach such as foreseeable consequences and reasonable behavior could be sent to the jury as in conventional negligence litigation. Damages would be difficult to quantify and might well be limited to actual losses.[149]

When the "use" of the data is to inform rather than to harm or to enrich, statutory mandates, common-law privileges and constitutional guarantees should serve as defenses to tort claims. Although case law on common-law privileges for invasion of privacy is sparse, they are usually treated as a fortiori available since they are presently invokable for *untrue* statements or misleading depictions.[150] To the extent remedies are created by statutes, conduct of data compilers, custodians and users can be additionally shaped and protected.

Practitioners and courts should remain alert to recognize the application of existing remedies from a variety of areas[151] to handle information misuse claims. Legislators can play vital roles in creating new rights, safeguards, and remedies where the existing patchwork is inadequate to cope with misuses. When legislation is attempted, it must be thoughtfully conceived and skillfully drafted to accomodate the complex social and economic interdependencies. To further aggravate the problem, the political and emotional conflicts in this area are potentially large and distracting. Information and communication are vital to our economy and the preservation of our heritage of democratic government and personal freedom. Protection for personal privacy is another, at

148. Identification can be based on voice-prints, fingerprints and social security numbers as well as names. There would seem little need for this duty to continue after the death of the file subject. *Cf.* Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).

149. Out-of-pocket expenses and lost profits or net income losses should be recoverable, but dignitary losses and general damages might be inappropriate.

150. *See* text accompanying note 21 *supra.*

151. *See, e.g.*, 15 U.S.C. § 78p (1970) (securities law violations).

times conflicting, cherished and constitutionally recognized objective.[152] Vigilance, even-handedness, realism, and creativity will be required of the bar, the bench, and the legislatures to control successfully the misuse of information.

152. *See, e.g.*, Dietemann v. Time, Inc., 449 F.2d 245 (9th Cir. 1971) (investigative journalist intruding under subterfuge). *See generally* Note, *On Privacy: Constitutional Protection for Personal Liberty*, 48 N.Y.U.L. REV. 670 (1973).

APPENDIX

Following is a proposed statute drafted by the author relating to the use, monitoring, and dissemination of criminal justice records, intelligence material, and related data. Sections relating to legislative purpose, preamble, enacting clause, fiscal provisions, saving and severability clauses, and effective date are not included. A short title might be "Criminal Justice Data Security Act of 197_."

TABLE OF CONTENTS

Section 1. *Definitions.*

As used in this Act:

(1) "Individual data compilation" means data stored in an information system or the output of such a system, whether disseminated or communicated externally or not and whether in total, edited, encrypted, excerpted, abbreviated, or summarized form, so long as it is or can be retrieved or displayed by means of, is or can be communicated in conjunction with, or is or can be read, utilized, manipulated, or understood in conjunction with an individual identifier, including but not limited to name, fingerprints, or voice prints (or alphabetic or numeric codes derivable therefrom), social security number, or other identity referent.

(2) "Information system" means a system, whether manual, mechanical, electronic, magnetic, or a combination of said types, capable of and used in whole or in part to collect, process, store, retrieve, display, generate, compile, or disseminate individual data compilations which is owned, funded, or operated by or on behalf of, or the outputs of which are used in whole or

in part by any governmental agency of the State or its political subdivisions.

(3) "Criminal justice information" means information about an individual collected, generated, or disseminated as a result of an arrest, a receipt into custody, detention, initiation of or prosecution of proceedings before an arraigning magistrate, a grand jury, or a court of criminal jurisdiction by a criminal justice agent, including arrest record information, conviction record information, and correctional and release information. The term shall not include statistical or analytical reports or records in which individuals are not identified and from which their identities are not readily ascertainable or reasonably inferrable. The term shall not include criminal justice intelligence material, missing persons data, wanted persons information, presentence report information (except to the extent such a report contains factual summaries, excerpts or quoted material from data included in the definition of criminal justice information), or records of violations of local building or fire codes (excluding the crimes of arson or attempted arson).

(4) "Arrest record information" means information concerning the arrest of, detention of, or commencement of criminal proceedings against an individual and, to the extent that a final disposition of the matter has been reached, the disposition consequent to each such arrest. A juvenile custody report not related to an arrest shall not be considered an "arrest record" for purposes of this statute.

(5) "Conviction record information" means information revealing that a defendant has pleaded guilty or *nolo contendere* to or has been convicted of any criminal offense and also includes information about the sentence imposed and any withdrawals or modifications of the plea. If an appeal is pending, indication of such pendency shall also be included and, if the appeal results in an affirmance of the conviction, an indication of that fact shall also be included in the definition.

(6) "Correctional and release information" means a record of factual occurrences concerning an individual and generated by a criminal justice agency or any other agency in conection with bail, with pre-trial or post-trial release proceedings (including habeas corpus), with detention in a correctional institution, or escape, release, or transfer therefrom, with detention in an institution for the criminally insane, with participation in any rehabilitation program with parole or probation and any violations or suspensions thereof. The term shall also include records of findings, conclusions, and sanctions, if any, in disciplinary proceedings against individual inmates for alleged infractions of rules of the institution where the individual was incarcerated at the time of the incident in question.

(7) "Wanted persons information" means information aiding in the identification of any person wanted on an outstanding arrest warrant or wanted for the contemporaneous commission of a felony. The term includes the charge for which the warrant was issued or the type of crime contemporaneously committed, information relevant to the individual's danger to the community, and such other information as may reasonably be thought to facilitate the regaining of the custody of the individual.

(8) "Missing persons data" means information identifying persons

believed to be missing and also includes information about last known address, occupation, and vehicle use or ownership.

(9) "Criminal justice intelligence material" means information or conclusions based on surveillance, hearsay, investigation, research, or deductive reasoning relating to (but not limited to) an individual's habits, behavior, associations, reputation, beliefs, declarations, actions, or participation in transactions when there is reason to suspect that the individual is involved in or has participated in criminal activity (including being a fugitive or an escapee) or is a national security risk. The term also includes military or alternative service or civil service records, medical, psychiatric, psychological test results, evaluations, diagnoses, and opinions from whatever source, and the suspicions and opinions of law enforcement, corrections, human resources, tax collection, pre-sentence investigation or probation personnel. The term also includes school truancy or disciplinary records, juvenile justice records, and records of the Family Services Division of the Department of Human Resources to the extent such material may be assembled in or retrievable from an information system. Nothing herein alters the confidentiality or public record status or "sealed" status otherwise applicable to such information pertaining to juveniles.

(10) "Disposition" means an unambiguous description of the action taken subsequent to an arrest by any criminal justice agency. The term shall include, but shall not be limited to, decisions not to refer the case against the individual to a prosecutor, the prosecutor's election not to commence criminal proceedings against the individual, the death of the individual prior to plea or trial, indefinite postponement and the reason therefor, acquittal, acquittal by reason of insanity or diminished responsibility, charge dismissed or case continued by reason of mental incompetency, guilty plea, nolle prosequi, no paper, nolo contendere plea, convicted, extradited, turned over to federal law enforcement authorities for disposition, pardoned, mistrial-defendant discharged, or executive clemency.

(11) "Disseminate" means to transmit information whether audibly, by writing, by electromagnetic or visual pulses or waves, by electric voltages or currents, by magnetic fields or domains, by printing, by photocopying, or by any other means of communication and whether in plain text, encrypted, or abbreviated.

(12) "Purge" means to permanently remove information from an information system so that there is no identifiable trace or vestige of such information and no indication that such information was removed.

(13) "Seal" means to preclude access to or knowledge about information contained in an information system except in conjunction with a subject review procedures as provided in Section 10; (b) authorized research as provided in Section 5; (c) a specific court order as provided in Section 8; or (d) a security verification random sample audit as provided in Section 11.

(14) "Criminal justice agency" means and is limited to:

(a) The Governor of the State or his or her delegate as he or she (1) is acting as commander-in-chief of the [State Police]; (2) is considering appointing or offering an appointment to a spe-

cific individual for a full-time, salaried office, judgeship, commission or other employment; (3) is considering selecting, nominating, appointing, or recommending a specific individual for the position of mediator, conciliator, or arbitrator in a collective bargaining dispute involving public employees; (4) is hearing, or has appointed a specific delegate to hear in his behalf, an administrative appeal under Sections 8(6) or 10(13).

(b) The judges of the courts of criminal jurisdiction in this State, including juvenile courts hearing criminal charges, and the staff and employees of said courts;

(c) The Attorney General of this State and his or her deputies and staff;

(d) District Attorneys and their deputies and staffs;

(e) Law enforcement personnel employed by this State or by any of its political subdivisions;

(f) Employees of the Corrections Division of the Department of Human Resources of this State [or equivalent agency];

(g) A member of the State Board of Parole and his or her staff;

(h) Any employee of any state or local agency designated by the Governor as provided in Section 5;

(i) The operators or custodians of an information system containing or handling criminal justice information or criminal justice intelligence material.

(15) "The administration of criminal justice" means any activity by a governmental agency or individual personnel thereof involving the apprehension, detention, pre-trial release, post-trial release, prosecution, defense, or rehabilitation (including periodic interviews by probation or parole officials and release or escape data under any applicable statute of this State) of accused persons or criminal offenders or involving termination of parental rights or placement of children in foster homes or therapeutic, rehabilitative, or punitive treatment of persons convicted of or pleading guilty to criminal offenses involving intoxication or being under the influence of drugs or involving the collection, storage, dissemination, processing (other than for transmission), securing, or usage of criminal justice information.

(16) "Hard copy" means a tangible, durable copy, whether visually interpretable or not, which can exist outside of the information system.

(17) "Audit entry" means a record identifying specifics concerning incidents of access, input, processing or manipulation, or output involving an individual data compilation in a given information system as provided in Section 9 herein.

Section 2. *Access and Utilization by Criminal Justice Agencies.*

(1) An employee of a criminal justice agency shall have access to criminal justice information and criminal justice intelligence material con-

tained in individual data compilations in information systems only when and to the extent that he or she has a need to know based on (a) a current and ongoing role in the administration of criminal justice involving, in some substantial manner, the subject of the compilation; or based on (b) a role in the administration of personnel, hiring, internal review, or employment benefits involving the subject of the compilation.

(2) Any person accessing individual data compilations containing criminal justice information or criminal justice intelligence material in an information system shall record in the system (or cause the system to record) the date of access, the agency employing him or her, the person's own identifying number, whether or not hard copies were made or received and, if any information was input to the system, a designation of the type or types of information as defined in Section 1(4)-(9). Uniform codes or abbreviations may be developed to facilitate such recordation.

(3) If any person accessing an individual data compilation containing criminal justice information or criminal justice intelligence material in an information system procures, generates, or receives a hard copy, or generates an excerpt, paraphrase, condensation, or like summary in hard copy form, he or she shall be responsible for either returning the hard copy to a secure manual information system or else destroying said copy when his or her need for it has terminated. In the event it is necessary to transfer custody of the hard copy to another individual authorized by law to keep, view, use, or access said copy, the first person shall promptly record the details of such a transfer in the information system. The transferee shall then succeed to like responsibility for future return, destruction, or transfer. In no event shall any person make additional copies without recording with the information system the identity of the custodian of each such copy and without informing the new custodians of the ongoing responsibilities inherent in possessing such copies. No dissemination hereunder shall be otherwise than in compliance with Sections 2, 3, 4, 5, 7, and 11 of this Act as they may respectively apply.

Section 3. *Access and Utilization for Out-of-State Criminal Justice Agencies.*

(1) Agencies of other states or nations performing functions equivalent to those performed by agencies in this State designated as criminal justice agencies may have access to or be recipients of individual data compilations containing criminal justice information stored or collected by an information system; provided that:

(a) They declare they have a need to know based on the administration of criminal justice involving, in some substantial manner, the subject of the data; and

(b) An audit entry is created in the individual data compilation of the subject in a manner consistent with Section 9(3) herein.

Such agencies may also have access to or be recipients of individual data compilations containing criminal justice intelligence material if, in addition to the above requirements, they declare either:

> (c) That the subject individual is wanted in their state as a fugitive or escapee and his or her whereabouts is either unknown or known to be in their state; or
>
> (d) That the subject individual has applied for a job with an agency of their state performing the functions of a criminal justice agency and the applicant has provided them with a written waiver allowing them to request, receive, and utilize such information.

Whenever an out-of-state agency otherwise eligible to access or receive such information has a direct link to an automated or computerized information system, the Attorney General of this State shall condition such direct link on the existence of an agreement by the out-of-state agency involved that it is aware of the limitations specified herein, including the requisite need to know and will condition its access to the information system so as to always fully and simultaneously comply with the requirements of this section.

In all other cases and in the case of accessing criminal justice intelligence material, the agency accessing the information system or receiving the data therefrom shall provide the information system operators with a hard copy of the requisite declarations and identifiers contemporaneously with, or as soon as practicable following, the request for access to or for information from the information system.

(2) The Federal Bureau of Investigation, its Identification Division, the National Crime Information Center and federal non-military intelligence agencies may have access to, by direct link or otherwise, and may receive data from and input data to individual data compilations in an information system containing criminal justice information or criminal justice intelligence material; provided, that the agencies may only input to, access, or receive data from the information system in pursuance of their administrative criminal justice function in connection with a federal crime committed or alleged to have been committed by the subject of the data; or in connection with assisting state law enforcement authorities when the subject of the data is a convicted offender under the laws of more than one state or nation; or when the subject of the data is being considered for a security clearance of "secret" or higher or for a federal government office, job, or post requiring approval of one or both houses of Congress; or when the subject of the data is reasonably believed to constitute or is closely related to someone who is reasonably believed to constitute a threat to the national security. In no event shall any such agency input to, access, or receive data from such an individual data compilation when a purpose of such activity is to facilitate or accomplish political surveillance of or assemble a political dossier on the subject of the data or other persons mentioned therein.

The Governor of this State shall obtain the prior written agreement of all such federal agencies to comply with the above limitations and conditions upon input, access, and receipt of information. Once such agreement is obtained, individual certificates of compliance need not be required, al-

though an audit entry as provided in Section 9 shall be made for each such incident. Such written agreement shall be reaffirmed at periodic intervals which shall not exceed two years.

(3) Federal courts and employees thereof, U.S. Attorneys, and their deputies and staff shall have access to and may receive data from individual data compilations in an information system containing criminal justice information to the extent that data therein bears on the merits of any pending criminal grand jury, prosecution, pre-trial or post-trial release, habeas corpus proceeding, criminal appeal or sentencing within their jurisdiction.

Section 4. *Access and Utilization by Other Agencies.*

(1) An information system or its operating personnel may provide the conviction record information portion of an individual data compilation in hard copy or otherwise to:

(a) The State Department of Motor Vehicles [or equivalent agency] to the extent that data therein pertains to a vehicle code violation.

(b) The Fish and Game Commission [or equivalent agency] to the extent that data therein pertains to a violation of the State fish or game laws.

(c) The Liquor Control Commission [or equivalent agency] to the extent data therein pertains to violations of law concerning the sale, possession, or dispensing of alcoholic beverages.

(2) Personnel operating or having authorized access to an information system may make criminal justice information contained in an individual data compilation available to:

(a) Counsel of record in a pending indictment, prosecution or appeal therefrom, civil rights action, or habeas corpus proceeding, upon order by the court having jurisdiction over such proceeding;

(b) Officials of juvenile detention facilities, child welfare workers, and counselors in the Human Relations Division of the Department of Human Resources [or equivalent agency] when the individual concerned is the child or juvenile subject of a current or pending file or of ongoing detention or escape therefrom, or is a natural parent, guardian, potential guardian, foster parent, or potential foster parent of a child or juvenile who is the subject of a current or pending file; provided, the requesting party declares in a writing filed with and recorded in the information system that she or he has a need to know such information to adequately carry out her or his function and agrees not to disseminate the information beyond persons in the same agency with a similar need to know.

(3) Personnel operating or having authorized access to an information system may make certain information from the arrest record, conviction

record, and release-parole-probation record portions of an individual data compilation available upon request to specified would-be or actual employers strictly on the following basis:

(a) No data shall be disseminated, paraphrased, or summarized hereunder except upon the presentation and surrender of an original or certified copy of a written consent to such disclosure executed by the employee or job applicant indicating the identity of the corporate personnel manager, or the employer him or herself if it is not a corporation. The operators of the information system shall retain said consents in a hard copy file and shall input an appropriate audit entry to the information system;

(b) Any branch of the armed services of the United States or the State National Guard may receive all conviction records, arrest records, and correctional and release information pertaining to an individual who is attempting to enlist or reenlist or who has applied for a security clearance or a commission or is under charges for an infraction of military law; provided that in the latter case the consent required in subparagraph (3)(a) above need not be obtained;

(c) Banks, savings and loan associations, finance, and commercial loan companies may receive conviction record information to the extent it pertains to the crimes of embezzlement, forgery, theft, or narcotics sale or use and concerns an employee or a job applicant;

(d) Hospitals, pharmacies, clinics, infirmaries, convalescent homes, physicians, osteopaths, and chiropractors may receive conviction record and correctional information to the extent it pertains to crimes involving narcotics or dangerous drugs and concerns an employee or job applicant;

(e) Public or private schools may receive conviction record and correctional information to the extent it pertains to crimes involving narcotics or dangerous drugs or sexual behavior or to a determination of sexual psychopathy or criminal insanity and concerns an employee or a job applicant;

(f) Health spas, gymnasiums, reducing salons, athletic clubs and facilities, massage parlors, Turkish baths, children's camps, day-care centers, and park, recreation, and swimming programs may receive conviction record and correctional information to the extent that it pertains to crimes involving sexual behavior or to a determination of sexual psychopathy and concerns an employee or a job applicant;

(g) Issuers of bail bonds may receive correctional records pertaining to bail or pre-trial release status and conviction and arrest information concerning individuals who have requested them to post bail;

(h) Automobile insurance companies may receive conviction record information to the extent that it pertains to violations of the motor vehicle laws of this State without the need of the consent specified in Section 4(3)(a).

(4) To the extent that hard copies are disseminated under paragraphs (1) - (3) of this section, the recipient shall destroy such copies as soon as the need which justified the original dissemination has terminated. The recipient and its employees and agents shall not paraphrase, repeat, summarize, or otherwise communicate or disseminate beyond his or her fellow employees who share his or her need to know the information received under paragraphs (1) - (3) of this section. A reminder of these requirements shall be printed or stamped on the face of each page of any hard copies provided by the information system.

(5) Subject to such specific orders as the courts having jurisdiction might issue, the news media shall only have access to the pleadings and orders, decrees, verdicts, and sentences in court proceedings, and to daily arrest data, including names of arrestees, within twenty-four hours after the arrest is made, and to convection record information, prison release or escape information immediately following the most recent sentencing or decision or appeal therefrom, or the time of release or escape respectively.

(6) In the event that an appeal was pending when conviction record information was furnished or disseminated under Sections 2-4 of this Act and as a result of the appeal, the individual subject was acquitted or the case was reversed and remanded for further trial which is either pending or was not prosecuted or ended in an acquittal, these facts shall be promptly supplied to the agency to which the conviction record information was originally supplied. Nothing herein shall preclude criminal justice agencies or the individual being detained from notifying the individual's immediate family or his or her issuer of bail bonds of the individual's detention.

Section 5. *Agencies Specifically Designated for Access; Research.*

(1) The Attorney General may authorize access to criminal justice information by:

(a) State agencies when the information is required by the agency to perform a duty or function expressly required by statute; and

(b) Other persons or organizations for purposes of programs of research in state criminal justice agencies.

(2) District attorneys may authorize access to criminal justice record information by:

(a) Local agencies and municipal corporations when the information is required to perform a duty or function expressly required by charter, ordinance, or statute; and

(b) Other persons or organizations for purposes of research at local levels.

(3) Whenever a district attorney authorizes access pursuant to subsection (2) of this section he shall promptly inform the Attorney General of the authorization to the agency and the character and condition of the authorization.

(4) When the Attorney General or a district attorney authorizes access to criminal justice information pursuant to this section, he shall:

(a) Make a specific finding of the duty and function requiring the access;

(b) Impose such conditions as may be necessary to preserve the system security and individual privacy; and

(c) Advise the agency, person, or organization of the liabilities attached to unauthorized dissemination of criminal justice information.

(5) Under this section authorization of access to other than criminal justice agencies by the Attorney General or a district attorney may be either:

(a) Access to information relating to specific criminal justice information on a single occasion; or

(b) A general grant of access. General grants may be for whole categories of criminal justice information for a specified period of time, not to exceed two years, and shall be required to be renewed with such specified period. In addition to other specifications and requirements, the authorization shall provide for the execution of nondisclosure agreements, audits, and shall specify the character of the criminal justice information the researchers may obtain.

(6) When the Attorney General or a district attorney authorizes access to criminal justice information for research purposes pursuant to this section, the authorization shall be conditioned upon:

(a) The execution of nondisclosure agreements by all participants in the research program; and

(b) The consultation and approval of the criminal justice agency or agencies maintaining the information system. However, criminal justice agencies shall not unreasonably withhold approval. The criminal justice agency may require the requesting party to reimburse the criminal justice agency for the cost of providing the authorized information; and

(c) Such additional requirements and conditions including a statement comparable to that required by Section 11 of this Act as he may find necessary to assure the protection of privacy and security interests.

(7) The Attorney General shall include in a biennial report to the legislature a report of all authorizations granted by him or by district attorneys pursuant to this section together with the character and conditions of the authorizations.

Section 6. *Wanted and Missing Persons.*

Wanted persons information and missing persons data may be stored in an information system, including an automated or computerized system, for only so long as the person is wanted or missing, and may be disseminated to law enforcement agencies, news media, and, in the case of missing persons, to private investigators working on behalf of the next of kin, or to the next of kin.

Section 7. *Representations by Rehabilitation Personnel and Judges.*

(1) Parole or probations officers or other persons employed by criminal justice agencies to assist in the social, occupational, or educational rehabilitation of convicted felons or juvenile offenders may, with the consent of the person under their supervision to whom it refers, orally represent the substance of the criminal justice information in any individual data compilation pertaining to said person to prospective employers, admission and scholarship officials of educational institutions, lending officials of financial institutions or private investors if such representation, in the judgment of such officers, would facilitate the rehabilitation of said person.

(2) A court in a criminal proceeding may disclose selected portions of criminal justice information pertaining to a party or a sworn witness in such a case in a published opinion or in the course of a public trial, hearing, sentencing, arraignment, or appeal.

Section 8. *Data to be Purged or Sealed.*

(1) Arrest record information shall reflect the disposition of the arrested person's case whenever a disposition has occurred except when entries pertaining to a specific arrest are required to be purged by court order or by operation of this or any other statute.

(2) In the case of any disposition which did *not* involve an acquittal, dismissal, or continuance all by reason of either insanity, diminished responsibility, or mental incompetence; a conviction, a nolo contendere plea, an extradition, a turn-over to federal authorities, a pardon or other exercise of executive clemency, the data pertaining to the antecedent arrest and to said disposition shall be purged from the individual data compilation in any information system. Bail forfeiture of under fifty dollars for traffic violations shall be treated as failures to prosecute if no further prosecution ensues.

(3) Any criminal justice agency or information system which originally disseminated data concerning an arrest in its jurisdiction to any criminal justice agency or other agency with similar function inside or outside the state or to any information system shall notify the recipient agency or system of the disposition following such arrest as soon as such information becomes available. If such disposition requires the purging of the original data then the originating agency shall notify the recipient agency or system of this fact and the reason therefor.

(4) Any information system receiving arrest record information to generate (or be added to) an individual data compilation within its control,

where such information does not include the disposition, shall query the originating agency regarding disposition no less often than every ninety days until such time as the disposition is received and either added to the compilation or data pertaining to the arrest incident is purged. Pending such clarification or purge, the information system shall record an entry generally understood to mean "no disposition as yet."

(5) If no disposition has been achieved within eighteen months of an arrest and the arrestee is not or has not been a fugitive on that or any other charge during said eighteen months, the data pertaining to that arrest shall be purged. If the information system is automated or computerized, purging under this section shall be done automatically.

(6) Any criminal justice agency desiring to itself continue to maintain arrest record information otherwise subject to purge or to have an information system continue to maintain such information may petition the Governor or his or her delegate for an exception to the purge requirement of this section. Upon receipt of such a petition the Governor or his or her delegate shall notify the subject of the arrest record information of his or her rights to and in connection with a contested case hearing to determine the propriety of continued maintenance of such information. The burden in such a proceeding is on the criminal justice agency to show a compelling public interest in maintaining such information. [An acquittal, dismissal, or decision not to prosecute the individual following his arrest based solely on lack of admissible corroborating evidence in conjunction with the constitutional inadmissibility (on search and seizure or due process grounds) of ostensibly probative and incriminating evidence, testimony, or confessions, may be evidence of a compelling public interest but need not be determinative of such an interest.] If the Governor delegates a person to act in his or her stead for the purpose of this section such a person shall not be or shall not have been active in law enforcement work and shall not be or shall not have been active in the criminal defense bar.

(7) Criminal justice information may be purged or sealed by order of a court having jurisdiction over such a matter or by operation of statute. If an item of information is to be sealed, it shall be sealed in all information systems in the state; and the court, if any, ordering the sealing, and the criminal justice agency that originally recorded the information, shall notify all information systems believed to contain the information of the fact that it should be sealed.

(8) In the event that the only data in an individual data compilation is an arrest record subject to purge under paragraphs (2) or (5) of this section and there has been no successful petition under paragraph (6) of this section, the purging shall be accomplished so that no trace remains of the individual's name or other identity referent.

(9) The provisions of subparagraphs (2), (3), (5), and (8) of this section shall not apply to "police blotters" and analogous arrest records maintained at the lowest adminstrative levels on a collective (non-compiled), daily basis.

Section 9. *Maintenance of Audit Trails; Details of Audit Entry.*

(1) All information systems shall maintain audit entries covering a period of time of no less than four years in the immediate past.

(2) To the extent that an information system or its personnel may transfer, disseminate, share, transmit, or input some or all of an individual data compilation stored in such system to another information system, it shall also transmit to the other system all audit entries appropriately identified with reference to the subject of each such individual data compilation or portion thereof. The receiving information system shall maintain such audit entry information in the same general manner as it shall maintain audit entries originating at such receiving information system.

(3) An audit entry shall be maintained by every information system for every incident (whether internal or external) of access, input, processing or manipulation, or output involving an individual data compilation (all or any of which are hereinafter referred to as "access incidents"). Each such entry shall be retrievable on the basis of the identity of the subject of the individual data compilation and shall contain, at the minimum:

(a) A designation of the type of information involved in such incident (including criminal justice intelligence information);

(b) The identity of the person initiating the incident, and the identity of his or her supervisor;

(c) The name of the agency by whom the person identified in (b) is employed;

(d) The date of the incident; and

(e) A designation of whether data was added to, deleted from, substituted, modified or processed, displayed, output, relocated, or additionally located (and, if relocated or additionally located, an identifying reference to the new or additional location must be included).

(4) If personnel operating an information system access the system internally and subsequently, using a hard copy or information generated by that access, disseminate the information externally, an audit entry for both the internal access incident and the external access incident must be generated and maintained in the information system.

(5) An access incident which is nothing more than a search by the computer in a computerized information system (or an identity check by operating personnel in a non-computerized information system) for the proper information in the course of generating, compiling, retrieving, or processing data on a *different* individual shall not require an audit entry.

(6) An access incident which occurs solely in the course of the generation of a statistical report or other analytical research during which and from the end result of which the identity of any one individual is not readily ascertainable or reasonably inferrable shall not require an audit entry. However, if such report or research is done by an agency or individual other than a criminal justice agency, under the provisions of

Section 5(6) of this Act, an audit entry shall be required. This audit entry may consist of a designation referring to the researching entity's identity and the specific authorization received under Section 5(5) and (6) of this Act.

Section 10. *Data Subject's Right to Review.*

(1) Any individual shall have the right to inspect wanted persons information, missing persons data, or criminal justice information and all available audit entries pertaining thereto in his or her own individual data compilation in an information system.

(2) Such inspection may take place at:

(a) The criminal justice agency of origin of specific portions of such information as to those portions; or

(b) A criminal justice agency having physical custody of all or a portion of such information as to the portion in such custody; or

(c) At any criminal justice agency (including facilities of the State Corrections Division) having access to an information system containing the individual's data compilation.

(3) Agencies at which such information may be inspected may prescribe reasonable hours and places of inspection and may impose such additional restrictions, including fingerprinting, as are reasonably necessary to assure the security of the information and to verify the identity of those who seek the inspection.

(4) The agency shall allow the individual's immediate family and/or attorney to participate in the inspection if the individual so requests. The agency shall provide a hard copy of the inspected information if the individual so requests. The agency shall provide a person experienced in interpreting the data and the audit entries to make explanations on the agency's premises when and where necessary for the individual's accurate understanding of the inspected or copied material. A record shall be maintained by the agency, and the identities of the inspecting parties and the interpreting personnel, and a report of the inspection shall immediately be sent to information systems to which or with which the agency has previously transmitted or shared data concerning the subject individual. The provisions of this law pertaining to challenges, requests, and appeals from denials of requests shall be provided by the agency to the individual at the time of the inspection.

(5) No audit entries or location references pertaining to criminal justice intelligence material shall be available for inspection or copying under this section.

(6) No individual may inspect or copy information under this section from the same information system sooner than 180 days from the time he or she last exercised such rights to inspect or copy unless he or she obtains a waiver from the official responsible for operating the information system. The granting of such a waiver shall be within the discretion of such official.

(7) If an individual, after inspection or copying of criminal justice information in an individual data compilation pertaining to himself or herself, believes such information to be an inaccurate, deceptive, or incomplete recital of historical fact, or believes that such information contains data prohibited by law, he or she may challenge the data and request specified corrections, deletions, or additions be made subject to the procedures specified herein.

(8) Such a challenge and request shall be made in writing within forty days after the date of the beginning of the inspection and shall be presented to the criminal justice agency or other agency of the State or its political subdivisions which originated or generated the challenged data. Such agency shall immediately inform all information systems to which or with which it has previously transmitted or shared data concerning the subject individual of the filing of a challenge and the date or dates of the entry or entries being challanged.

(9) (a) Immediately following a report of an inspection by an individual under this section, information systems shall add to the appropriate individual data compilation a review status designation generally understood to mean "subject review pending";

(b) If no challenge is reported to have been filed within the forty day period, information systems shall change the review status to a designation generally understood to mean "subject review completed without challenge";

(c) If a challenge is reported to have been filed within the forty day period, information systems shall change the review status to a designation generally understood to mean "subject challange pending re: entries of ————" with the dates of the challenged entries to be inserted in the blank space;

(d) After the challenge procedure has culminated in a final determination and after review has been completed or waived, the information systems receiving reports of such final determination shall change the review status to a designation generally understood to reveal the date of the final determination, its docket number, and the words "challenge denied," "challenge sustained," or "challenge partially sustained" as the case may be.

(10) Information systems receiving a report of a challenge sustained or partially sustained shall immediately change the relevant data to comport with the more accurate version produced in the final determination of the challenge. If material is to be deleted it shall be removed in such a manner that no person or machine can know, understand, or process the deleted material.

(11) If the agency to which the claim is submitted has neither sustained, partially sustained, or denied the challenge within thirty days following its submission, the challenge shall be deemed denied by that agency insofar as the procedure for further review is concerned.

(12) If the agency which originated or initially generated the informa-

tion is not within this State, the subject of the individual data compilation may pursue whatever procedures are appropriate under the law of the jurisdiction where such agency is located. If and when such agency makes a report of challenge or makes a final determination of the challenge and such final determination is reported by or verified by such agency to an information system in this State, such information system shall update the review status of the subject's individual data compilation and the compilation itself in accord with the requirements of paragraphs (9) and (10) of this section. The forty-day period for challenge shall not apply to this paragraph, and, if no report of final determination or no renewal of a "challenge pending" report is made within 220 days of the beginning of the inspection, the information system shall change the review status to a designation generally understood to mean "challenge denied" unless and until a contrary report is received, at which time the appropriate correction to the review status and the individual data compilation shall be made.

(13) If the agency to which the challenge is presented declines to carry out the request of the subject of the individual data compilation to such subject's satisfaction, he or she may file a written request for review by the Governor or his or her delegate. If the Governor delegates a person to act in his or her stead for the purposes of this section, such person shall not be or shall not have been active in law enforcement work and shall not be or shall not have been active in the criminal defense bar.

The Governor or his or her delegate shall, in each case in which he or she finds a colorable basis for the challenge, conduct a contested case hearing. The underlying merits of the decision or activity which is the subject of the record shall not be in issue; only the accuracy, completeness, deceptiveness, or the includability in criminal justice information of the description of the decision of activity shall be in issue.

The agency, the Governor or his or her delegate, or the reviewing court, as the case may be, shall notify the agencies operating the information systems involved of the determination concerning the challenge and the pendency of further review if and when any further review is initiated. When no further review is possible, or when further review is waived, the last determining entity shall notify the information systems involved that the determination is final. In all such determination or review proceedings, the burden of justifying the requested change shall be on the subject of the individual data compilation.

(14) If a change in the criminal justice information concerning a person is required by reason of a successful challenge, or any internal action by the originating agency or the operators of an information system, all criminal justice agencies, including those in other states and in the federal government to which the now-changed criminal justice information in that person's individual data compilation was transmitted within four years preceding the final determination requiring the change, shall be notified by the information system of the exact nature of the change and to whom it pertains. The subject of the individual data compilation shall be promptly provided with a hard copy of the corrected information. Nothing in this

paragraph shall preclude the subject of an individual data compilation from personally notifying recipients of the now-changed information who received such information more than four years before the necessity for the change was determined to the extent he or she knows the identity of such recipients. Upon such notification and verification from the appropriate information system, such recipients shall update their records to comply with the change.

(15) If a change in the criminal justice information concerning a person is required by reason of a successful challenge or any internal action by the originating agency or the operators of an information system, all non-criminal justice agencies or entities to which the now-changed criminal justice information in that person's individual data compilation was transmitted within two years preceding the final determination requiring the change shall be notified by the information system of the exact nature of the change and to whom it pertains. The information system, its employees and operators, the State, its political subdivisions, and their respective officials and employees, shall be immune from civil suit for invasion of privacy as a consequence of following the procedures or sending the notifications required by this section.

Section 11. *Administration; Security; Training Programs; Audits.*

(1) Each information system shall adopt reasonable procedures designed to protect the physical security of the system and its contents, to prevent the unauthorized disclosure of all information contained in the system, to facilitate the current and accurate revision of criminal justice information to include subsequently received data, and to provide a continuing education program in the proper use and control of criminal justice information.

(2) The Governor or a criminal justice agency designated by him or her shall, in the manner provided by the State Administrative Procedure Act, adopt such rules as may be necessary to implement this Act.

(3) Whenever it appears to the Governor that an agency or person has failed or refused to comply with this Act or with rules adopted pursuant to paragraph (2) of this section, the Governor may bring suit for injunctive relief in the name and on behalf of this State in the [circuit] court of any county of this state to enforce compliance with the Act or such rule. Upon a proper showing a permanent or temporary injunction shall be granted.

(4) All employees of criminal justice agencies entitled to maintain or receive criminal justice information and criminal justice intelligence material from information systems shall, as a condition of their employment, execute (no less often than every two years) a statement indicating that they are aware of the security and privacy requirements of this Act and regulations thereunder and have been instructed in the proper use and control of such information.

(5) No less often than every two years each information system shall conduct a random sample audit of the individual data compilations which were active (*i.e.* which had an access, input, processing or manipulation, or

output) involving criminal justice intelligence material within the preceding two years. Individual data compilations numbering no less than [one-tenth of one percent] of the total of such active compilations shall be examined in the course of each such audit. Audit trails in such audited compilations shall be traced and verified. Inaccuracies in coding, and violations of conditions of or restrictions on access, dissemination or input, and any other aspects of non-compliance with this Act shall be noted, corrected to the extent possible (including the sending of the notifications specified in Section 10(14) and (15) where appropriate) and brought to the attention of the responsible officials for such further action or reprimands as may be appropriate. A summary of the findings of the audit and the actions taken as a result of the audit shall be transmitted to the Governor within sixty days of the completion of the audit. The summary shall not mention the subjects of the individual data compilations by name or other identifier. Each such summary shall become a public record upon filing with the Governor.

Section 12. *Intelligence and Surveillance Data.*

(1) No automated or computerized information system shall contain, store, process, transfer, or disseminate criminal justice intelligence material or surveillance reports pertaining to any individual person. For purposes of this section a TWX, a teletypewriter, a MODEM device, an encryption or scrambling device, or a computerized message switching device belonging to a licensed common carrier of communications shall not be deemed an information system.

(2) No criminal justice agency shall collect or maintain information about the political, religious, or social views, associations, or activities of any individual, group, association, organization, corporation, business, or partnership unless such information directly relates to an investigation of past or threatened criminal conduct and there are reasonable grounds to suspect the subject of the information is or may be involved in such conduct.

Section 13. *Civil Actions; Criminal Sanctions.*

(1) Any person may institute an action against this State, its employees, its criminal justice agencies, or its political subdivisions, their criminal justice agencies and their employees, for his or her damages for any violation of this Act, and to restrain future violations. Such action shall be brought in the [circuit] court of the county in which the individual resides or in which the allegedly violating criminal justice agency is located; and

(a) If a violation of the Act is proven, the person instituting the action shall recover his actual damages or $1,000, whichever is greater, together with reasonable attorney fees and costs and disbursements incurred; and

(b) Upon a showing of a wilful violation of the Act, the person will also be entitled to punitive damages; and

(c) Recovery under this section against this State or its

political subdivisions shall be subject to the maximum limits specified in [the sovereign immunity waiver statute].

(2) In any proceedings brought pursuant to this section the chief administrative officer of the criminal justice agency from which the information was published or disseminated will be rebuttably presumed to have authorized the dissemination contrary to this Act by his agent or employee and may be jointly and severally liable with the employee or agent.

(3) Information that is merely erroneous in content but is not maintained or disseminated in violation of this Act shall not cause any defendant to be liable in an action brought under this section unless the defendant or its agents wilfully and knowingly caused the content to be erroneous, or recklessly disregarded its erroneous nature after gaining actual knowledge that it was in error.

(4) Nothing in this Act shall prejudice, preempt, alter, or preclude whatever rights a person who is the subject of any individual data compilation may have under common law or statute:

(a) To sue another person or entity for defamation; or

(b) To sue a person who is not connected with, acting for, or employed by a criminal justice agency and who knowingly obtained, used or disseminated information concerning such individual that was or is contained in an information system in violation of this statute or of any other law.

(5) Any person who wilfully requests, obtains, or seeks to obtain information in any manner except in accordance with this Act, or who wilfully communicates or seeks to communicate criminal record information to any agency or person except in accordance with this Act, or any person who wilfully falsifies criminal justice information, criminal justice intelligence material, or any records relating thereto, shall be guilty of a misdemeanor.

Section 14. *Amendments to Other Statutes.*

[It may be necessary in any given jurisdiction to amend, concurrently with the enactment of this statute, other statutes already in force. For example, statutes conferring record keeping authority on state and local police may require modification. Similarly, public records statutes and freedom of information laws may require alignment with this statute. The civil sanctions sections may require alteration of the waiver of governmental immunity laws.]