"THE FILES": LEGAL CONTROLS OVER THE ACCURACY AND ACCESSIBILITY OF STORED PERSONAL DATA

KENNETH L. KARST*

In our record-keeping civilization,[1] the man whose name is not inscribed on the tab of someone's manila folder simply does not exist. Each of us, from the day he is born, begins to deposit information about himself in various public and private files. By the time he emerges from school and the armed forces, the ordinary young adult cannot have escaped becoming the subject of at least a dozen personal information files.[2] Our increasing social interdependence assures an acceleration of the rate at which personal data are accumulated and stored.

An impressively detailed profile of any individual can be drawn from files that are open to public inspection. But the investigator need not stop there; if he is talented, he will have access to a number of sensitive-information files that are normally thought of as confidential. The result is that anyone with money to spend on the project can secure a remarkably comprehensive personal history for any "subject"[3] he chooses to investigate.

Almost all this information has been supplied by the subject himself, willingly enough, as he has sought a job, or a loan, or an insurance policy. What he may not have understood is that each of these files generates information for other files. Not only is there no assurance that personal information will be used only for the

* A.B. 1950, University of California, Los Angeles; LL.B. 1953, Harvard University. Professor of Law, University of California, Los Angeles.

I should like to thank all those who have been generous with their time and counsel during the preparation of this article, including some who prefer not to be mentioned. In particular, I am grateful to the Honorable Jerome R. Waldie, former Majority Floor Leader of the California Assembly and now Congressman-elect; the Special Committee on Science and Law of the Association of the Bar of the City of New York, Oscar M. Ruebhausen, Esquire, Chairman; Mr. Eldridge Adams, of the UCLA Law-Science Center; Dr. Paul Baran, of the RAND Corporation; Earl Osadchey, Esquire, Special Assistant to the District Attorney, County of Los Angeles, California; and my colleagues, Professors William D. Warren and Robert L. Jordan.

[1] The characterization is no exaggeration. It is comforting to know that the First National Bank of Boston has built a bomb shelter for its own bank records and those of other members of the Boston Clearing House Association. The previously established storage center was too close to Westover Air Force Base, "a prime target in the event of an enemy attack," and so the new shelter was built in Pepperell, "to specifications estimated to protect the vault if a twenty megaton bomb struck anywhere outside of a three-mile radius." *Boston Bank Builds Big Foxhole*, N.Y. Times, Dec. 2, 1960, p. 41, col. 5.

[2] The following is a minimum list: birth record, hospital record, doctor's file, school files (at least three), Social Security records, tax records (probably more than one), driver's license records, employers' files, military records (several), fingerprints in the FBI's civil (non-criminal) files.

[3] This impersonal term is used throughout the article to indicate the person who is listed or described in a personal data file. With respect to the ease of access suggested in the text, see VANCE PACKARD, THE NAKED SOCIETY ch. 11 ("The Lively Traffic in Facts About Us") (1964) and particularly Mr. Packard's price list for "confidential" personal data: arrest record, $10; credit report to nonsubscriber, $5 or $10. *Id.* at 192.

purpose for which the subject submitted it; there is the opposite probability that it will be passed on and on. Investigators cooperate with each other, to their mutual advantage and to the advantage of the whole investigative system, from the Diners Club to the rogues' gallery.

This easy exchange of information is common even now, before the various investigative agencies have gone very far in adapting to recent advances in the technology of data processing. What the computer now makes possible is a substantial reduction of the time and the marginal cost required for the investigation of any one subject. At this midway point between *1984*[4] and 1984, a new image has been coupled to that of Orwell's closed-circuit television camera: it is the image of the electronic data bank, where a complete dossier for every one of us is literally at the fingertips of the console operator.[5]

Other contributions to this symposium have examined a number of reasons why that image is a disturbing one. Although there is only partial agreement as to the purposes and ultimate importance of various kinds of privacy,[6] it is possible to identify two broad classes of objectionable disclosure which legal institutions might seek to minimize. First, information out of a personal data file may be disclosed to an improper person. Second, such information may be false, or incomplete, or disclosed in a misleading way, so that its recipient receives a mistaken impression of the subject of the file. While the two problems of access and accuracy may overlap in a single factual context, they raise divergent questions for the legal system, and they deserve separate treatment.

Reversing the usual common law order of analysis, this article moves from the general to the particular. After considering some recurrent issues inherent in any system that attempts to restrict access to sensitive information in storage, or to police the accuracy of the information which is stored, the article examines in greater detail the manner in which those issues are raised in the contexts of law enforcement records and credit information files.

I

THE ANALYTICAL FRAMEWORK

A. Limitations on Access

Hardly anyone in our society can keep altogether secret very many facts about himself. Almost every such fact, however personal or sensitive, is known to someone

[4] George Orwell's book was published in 1949.

[5] One comprehensive list of types of personal data which will soon be stored on computer tapes takes six pages to *list*, with only the briefest description of some of the items. EDWARD F. R. HEARLE & R. J. MASON, A DATA PROCESSING SYSTEM FOR STATE & LOCAL GOVERNMENTS 118 (1963).

[6] See Ruebhausen & Brim, *Privacy and Behavioral Research*, 65 COLUM. L. REV. 1184, 1189 (1965): "to protect ourselves, or our process of creativity, or our minority views, or our self-respect"; VANCE PACKARD, THE NAKED SOCIETY 12 (1964): "the right to be different . . . to hope for tolerant forgiveness . . . to make a fresh start." An exceptionally thoughtful recent analysis of the functions of privacy is in

else. Meaningful discussion of privacy, therefore, requires the recognition that ordinarily we deal not with an interest in total nondisclosure but with an interest in selective disclosure.[7] Our concern is with *unauthorized* access to the files, and so we begin with an assumption, built into our definition of privacy: consent by the subject of the file excuses the disclosure of information about him. The assumption finds support in the growing case law of privacy. Not only is consent uniformly considered an effective defense to an action for damages for invasion of privacy;[8] it is also implicit in the very definition of unreasonable publicity: if the plaintiff has left the information "open to the public eye,"[9] he cannot complain when it is publicized.

Such a definitional technique, reading consented-to disclosures out of the law's concern, has ancient precedent in the maxim *volenti non fit injuria.* But it carries with it the danger that serious issues of policy may be resolved by question begging. One such issue relates to the reality of the freedom of choice exercised by the subject who makes his own disclosure of personal data. One who needs a job may choose to fill out the employer's questionnaire in preference to continued unemployment; during a housing shortage, a prospective tenant may choose to respond to the landlord's questions. While such disclosures may fit within a legal conclusion labeled "consent," the circumstances under which they are initially made may cause us to lean toward a strict limitation on their transmission to other investigators with other purposes.[10]

A second danger in basing analysis on consent lies in the seductiveness of notions about "implied consent." A recent article on the implications for privacy of research in the behavioral sciences draws an analogy to the "public figure" cases in the following terms:

Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's—Part I,* 66 COLUM. L. REV. 1003, 1017-40 (1966), published as this article went to press.

[7] See Ruebhausen & Brim, *supra* note 6, at 1188-90. The interest in selective disclosure may be the one important feature shared by the common law right of privacy and the proprietary interest in publicly exploiting one's own personality. See Nimmer, *The Right of Publicity,* 19 LAW & CONTEMP. PROB. 203 (1954).

[8] Dean Prosser has collected the cases. Prosser, *Privacy,* 48 CALIF. L. REV. 383, 419-21 (1960), reprinted in WILLIAM L. PROSSER, TORTS 850-51 (3d ed. 1964). The rule follows a fortiori from the same defense to defamation. See 3 RESTATEMENT, TORTS § 583 (1938).

[9] Prosser, *Privacy,* 48 CALIF. L. REV. 383, 394 (1960).

[10] The case for restricted access is strongest when the information has been coerced from the subject of the file. Yet in St. Regis Paper Co. v. United States, 368 U.S. 208 (1961), the Supreme Court affirmed a decree ordering the paper company to furnish to the FTC its file copies of certain reports which it had been required to make to the Census Bureau, despite the statutory provision, 13 U.S.C. § 9(a) (1958), forbidding the Commerce Department to use the material for other than statistical purposes or to permit others outside the Department to examine individual reports. At its next session, Congress amended § 9(a) to forbid other federal agencies to require census reports or file copies. 76 Stat. 922 (1962), 13 U.S.C. § 9(a) (1964). See *Hearings on Confidentiality of Census Reports Before the House Committee on Post Office and Civil Service,* 87th Cong., 2d Sess. (1962). There is no doubt that the information must be given to the Census Bureau. See United States v. Rickenbacker, 309 F.2d 462 (2d Cir. 1962), *cert. denied,* 371 U.S. 962 (1963).

> Certainly, public figures, particularly those who appeal to the public for elective office, have impliedly consented to the yielding up of some areas of private personality. The comings and goings of a Mayor or Governor, or Hollywood starlet, and a public evaluation and discussion of their strengths and weaknesses in their public roles are proper subjects of news reports, analysis and research.[11]

Two different ideas are expressed in this passage. Its first assumption, that the decisions denying public figures damages for invasion of privacy are based on a consent theory, is surely mistaken. If the mayor or the starlet were expressly to withhold consent to publication, the result would not be changed. The second part of the quoted passage would still be valid: their doings as public figures would still be "proper subjects" for treatment in the press. The reason is not that they have consented to the publicity but that publicity is *justified* in the public interest, whether or not they consent.[12]

One reason why analysis on the basis of a consent principle may be attractive is that it seems to relieve courts and other policy makers from making the difficult determination of the kinds of information that ought to be kept confidential. In theory, a principle of consent leaves such choices to the subject of the file. That analytical advantage, however, is illusory; the result of describing these issues of justification for disclosure as if they were issues of consent is that it obscures the real basis for decision. The utility of such a fiction has not been demonstrated.

To say that the consent principle disposes of little more than the easy cases relating to access to sensitive personal data is not to deny the principle's importance. A great many, perhaps a majority, of such disclosures are made under circumstances that can be described as easy cases. The more challenging questions for the legal system, however, are raised by claims of access to such information in the absence of the subject's consent, or even over his protest. Here the task is to give legal content to the expression, "None of your business."

In a variety of contexts, our courts and legislatures have already struck a series of legislative balances between individual interests in privacy and countervailing interests in the free exchange of information. In seeking a clearer understanding of those interests, we may find guidance in the law of defamation, in the more recently developed common law of invasion of privacy, and in legislation and judicial decisions defining those governmental records which are "public." The diverse issues raised in all these cases can be tied together artificially under some conclusory slogan like "need to know,"[13] but the recognition of some common features should not produce the hasty conclusion that the issues should be decided in the same way.

Although our present concern is not with inaccuracies in files of personal data, a number of the privileges established in the law of defamation are instructive. The

[11] Ruebhausen & Brim, *supra* note 6, at 1199.

[12] Messrs. Ruebhausen and Brim recognize that consent is not the only operative principle in this context. See *id.* at 1201-04.

[13] The phrase comes from the various government security manuals, which leave it undefined.

qualified privilege[14] to make a defamatory statement in order to protect the interest of the recipient of the statement, or a common interest of speaker and recipient, has been applied to many situations of the type with which we are concerned. Thus, a disclosure of information out of the subject's personal data file to a prospective employer's investigator, or to a credit investigator, or to a policeman, would be privileged.[15] The privilege does not extend, however, to the publication of "defamatory matter not reasonably necessary to accomplish the purpose of the occasion"[16] or to persons who have no interest in the subject matter of the communication.[17] While these formulations amount to little more than saying that publication is justified when it is justified, they do help us to identify two complementary aspects of the "need to know" problem: the nature of the information disclosed and the persons to whom disclosure is made. A system of limitations on disclosure might attack either of these aspects, or both.

A parallel set of two limiting factors has been built into that portion of the tort law of privacy which Dean Prosser calls the "public disclosure of private facts."[18] First, the facts disclosed must be of an intimate or private nature and not facts that are available to one who inspects records open to the public.[19] Second, the facts must be disclosed to the public or at least to a large group.[20] These requirements, like the limitations on the qualified privilege in defamation cases, relate to the type of facts disclosed and to the persons who receive the disclosures. They represent, however, a shift of concern from one side of the policy balance to the other. In the defamation cases, the existence of the privilege depends on the presence or absence of justification for a concededly harmful disclosure. In the privacy cases, it is the degree to which the disclosure has resulted in harm that is in question.[21] The evalua-

[14] The privilege is qualified, and not absolute, in that it can be lost if the publication is shown to have been made with "malice," *i.e.*, either an intention to injure or knowledge of the statement's falsity. Recklessness is generally held to be the equivalent of such knowledge, but negligence is not.

[15] See the entertaining discussion of the cases in CHAS. O. GREGORY & HARRY KALVEN, JR., CASES ON TORTS 1007-14 (1959).

[16] Sheehan v. Tobin, 326 Mass. 185, 194, 93 N.E.2d 524, 530 (1950), paraphrasing RESTATEMENT, TORTS § 599, comment *a* (1938).

[17] *E.g.*, Pollasky v. Minchener, 81 Mich. 280, 46 N.W. 5 (1890) (business reporting agency not privileged to send derogatory report concerning plaintiffs to subscribers who had not inquired about them).

[18] Prosser, *Privacy*, 48 CALIF. L. REV. 383, 392-98 (1960).

[19] In one unusual case, however, a public record of an old criminal conviction was held to be unreasonably publicized to the plaintiff's present acquaintances. The plaintiff's rather lurid past, her intervening reformation, and her successful change of identity may limit the application of the decision to other cases. Melvin v. Reid, 112 Cal. App. 285, 297 Pac. 91 (Dist. Ct. App. 1931).

[20] Typically, the defendants come from the mass communications media. *But cf.* York v. Story, 324 F.2d 450 (9th Cir. 1963) (defendant police officer's circulation among police personnel of photographs of plaintiff in indecent positions, taken over plaintiff's objections, violates the right of privacy guaranteed by the due process clause of the fourteenth amendment, justifying damages action under Civil Rights Act). See Peterson v. Idaho First Nat'l Bank, 83 Idaho 578, 367 P.2d 284 (1961), discussed in note 146 *infra*.

[21] Of course, many privacy cases also raise questions of justification, under the doctrinal heading of "newsworthiness." Warren and Brandeis, in their famous article, *The Right to Privacy*, 4 HARV. L. REV. 193, 216 (1890), assumed that the defamation privileges would apply to actions for invasion of privacy. Many of those privileges, however, have been swallowed up in the question of the reasonableness of the publication.

tion of a recipient's "need to know" should thus be particularized into several narrower, more manageable inquiries. That particularization will produce no universal formula for decision, but it will promote a careful consideration of the interests at stake in the various factual contexts with which the law must deal.

The established tort doctrine relating to our problem may be summarized as follows: If accurate information is disclosed out of the subject's file, there is no liability unless disclosure is made to a great number of people, however sensitive the information may be. Since disclosure of such information is normally made only to professional investigators, the remedy of damages for invasion of privacy offers little protection to the subject. And even though the information be arguably false, the disclosure will be qualifiedly privileged against an action for damages on a defamation theory so long as the investigator is, or represents, a prospective lender, a wife seeking evidence in a divorce proceeding, a prospective insurer, or someone else who has what the law regards as a sufficient interest in inquiring—assuming that the information disclosed is relevant to that interest. The kind of rigid limitation on access to sensitive personal information that would be needed in order to give the subject effective protection against improper disclosure of personal data is thus uncongenial to existing theories of recovery of damages for defamation or invasion of privacy.[22]

Meager as it is, however, the law of torts is at present the principal legal protection against unjustified access to data in nongovernmental files, such as those to be found in the offices of credit associations, insurance companies, and private hospitals. Government repositories, on the other hand, are often obliged by statute to limit access to their files. While the controlling legislation typically includes a general provision that "public records" or "public writings" are freely available for inspection[23] and some records are specifically identified by statute as public, other legislation makes certain government files "confidential," open only to officials directly concerned with the administration of the programs that have motivated the gathering of the information.[24] Often, however, there is no express statutory directive to the

[22] With respect to injunctive relief, see text accompanying note 40 *infra*.

[23] *E.g.*, CAL. CIV. PROC. CODE § 1892: "Every citizen has a right to inspect and take a copy of any public writing of this State, except as otherwise expressly provided by statute." This provision, in its present form, was enacted as part of the original code in 1872. CAL. GOV'T CODE § 1227 extends to "any citizen" the right to inspect "public records and other matters in the office of any [state] officer, except as otherwise provided . . . ."

Similar legislation, applicable to federal agencies, was adopted by the Congress in July 1966. "Identifiable" agency records are to be made available on request, and the right to inspect is enforceable in a federal court. Excepted from this provision, among other records, are: "Personnel and medical files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy," and "investigatory files compiled for law enforcement purposes except to the extent available by law to a private party . . . ." The provision amends section 3 of the Administrative Procedure Act, 5 U.S.C. § 1003 (1964).

[24] See Comment, *Inspection of Public Records Under California Law*, 50 CALIF. L. REV. 79 (1962). The author of the comment identified 88 statutory prohibitions or restrictions of disclosure of state records, 78 of which "deal with records relating primarily to the private and business affairs of individuals and corporations." *Id.* at 82 n.18. One such provision relates to reports of "disorders characterized by lapses of consciousness," which must be made by the physicians who diagnose such disorders. The reports are made to the local health officer, who passes them on to the State Department

custodian of government files. In such a case, the courts must decide whether the record is public—usually at the request of a citizen, sometimes a newspaper reporter, who asserts that the custodian's refusal to open the records is a denial of "the public's right to know" about the operation of its government. In that context, it is not surprising that a number of decisions recognize a presumption that a record is public.[25] All that such a rule means is that the court will decide in favor of free access to the records unless the custodian makes a convincing argument to the contrary, but the presumption is nonetheless an accurate expression of the tendency of the decisions to favor free access to information in the government's hands.[26]

No constitutional problem is raised, then, by a statute that makes public even highly sensitive personal information in the government's files.[27] Indeed, there may be some constitutional limits on the power of a legislature to *forbid* disclosure, in cases in which the information relates closely to the conduct of the government's business. Mr. Justice Black, concurring in the libel case of *Barr v. Matteo*,[28] made this comment:

> How far the Congress itself could go in barring federal officials and employees from discussing public matters consistently with the First Amendment is a question we need not reach in this case.

---

of Health, for use by the State Department of Motor Vehicles. The reports are to be "kept confidential and used solely for the purpose of determining the eligibility" to drive an automobile. CAL. HEALTH & SAFETY CODE § 410. Similar protections of confidentiality appear in some "battered child" statutes, which require doctors to report such cases to a state investigator. The investigator's files are normally accessible only to welfare and law enforcement agencies. See McCoid, *The Battered Child and Other Assaults Upon the Family, Part I*, 50 MINN. L. REV. 1 (1965).

Often, even "confidential" records are available to official investigators from other agencies. For example, a number of congressional committees, including the House Committee on Un-American Activities, have had access to federal income tax returns. One official list appears following INT. REV. CODE OF 1954, § 6103; the authorizations are periodically renewed. See also 12 C.F.R. § 4.13(b) (1965), in which the Comptroller of the Currency, partly to protect the interest of banks and their customers in privacy, has declared his investigative records and other sensitive data records confidential, but with the proviso that certain U.S. government agencies may have access to the information on conditions to be imposed by the Comptroller.

[25] One leading decision which does not use the language of presumptions but which nonetheless reasons in that manner is Egan v. Board of Water Supply, 205 N.Y. 147, 98 N.E. 467 (1912).

[26] Exceptions are made for "state secrets" and other forms of governmental privilege, based on a *public* interest in confidentiality, as in cases involving disclosures made to investigative officers in confidence. See Comment, *supra* note 24, at 84-87.

[27] Or by a statute giving discretion to the custodian of governmental records to decide on the types of information which will be made public. In Hubbard v. Mellon, 55 App. D.C. 341, 5 F.2d 764 (1925), it was held that there was no enjoinable constitutional violation in a statute authorizing the posting in the office of each internal revenue collector's office of the names and addresses of taxpayers, together with the amounts of tax paid by them. When a Kansas City newspaper reprinted such a list, its owners were indicted for violating the statute prohibiting publication of "any income return, or any part thereof . . . ." The prohibition was qualified by the language, "in any manner not provided by law," and the Supreme Court affirmed a dismissal of the indictment, holding that the authorization to the collector protected the editors. United States v. Dickey, 268 U.S. 378 (1925). The information, said the Court, could not "be regarded otherwise than as public property, to be passed on to others as freely as the possessors of it may choose." Furthermore, "the wisdom, on the one hand, of secrecy, and, on the other hand, of publicity, in respect of tax returns," was said to be "addressed to the discretion of the lawmaking department . . . ." *Id.* at 386-87.

[28] 360 U.S. 564, 577 (1959).

The key to any such constitutional principle no doubt lies in the phrase "public matters," which can be distinguished from "purely private libels, totally unrelated to public affairs."[29] It is not suggested here that all the rules of privilege in public-affairs libel cases are or should be constitutional rules; within the limits of the Constitution surely there is some room for legislative choice, in the establishment of defamation privileges as in the selection of certain records to be open to the public. But in striking any of these balances, the same questions must be asked which we identified in discussing the common law remedies for defamation and invasion of privacy: In what respect might disclosure of the information injure the reputations or emotional tranquility or economic interests of the class of subjects in question? Are other sources for the same data readily available, so that *this* disclosure is of minor importance? Is the disclosure limited to a few recipients? If so, are the recipients in a position to use the disclosed data to deny the subject a benefit, or to impose some sanction on him? Is that benefit or sanction a significant one? Are the data relevant to the investigative objectives of the recipient? To what extent will the information be of significant value to him in the protection of his, or his client's, interests? Are those interests and those objectives worthy of the law's assistance?

These final questions of justification and relevance take us far down the road toward a definition of the kind of society we want. Here, as in the law of evidence, relevance depends on the context of the inquiry. We know that a prospective employer may very well want to be informed of the drinking habits of a prospective executive's wife.[30] But *should* that information be passed on to him? Does not the answer to the latter question depend on the views of the policymaker on the propriety of considering such factors in the hiring process?

At this point in the analysis we face an issue of competence: Who should decide such questions of relevance? The first amendment is a promise that, to a very great extent, each participant in the interchange of communications shall be the judge of his own "need to know." To a very great extent, but not completely, a rule, constitutionally imposed or otherwise, conferring a freedom of unlimited investigation would be just as unacceptable an absolute as would a pure consent rule conferring control over all disclosures of personal data on the subject of the data. As Chief Justice Warren recently said in a quite different context, "The right to speak and publish does not carry with it the unrestrained right to gather information."[31]

Between those polar absolutes, legislators, judges, and the custodians of public and private records have the responsibility to make informed choices of community policy. It should be obvious that these choices cannot easily be separated from the views of the decision makers as to the relative value of various aspects of individual

[29] The quoted phrase in Mr. Justice Brennan's, in Garrison v. Louisiana, 379 U.S. 64, 72 n.8 (1964), discussed in text accompanying note 46 *infra*.

[30] See Burns, *The Private Investigative Agency and Privacy Intrusions*, in THE RIGHT OF PRIVACY, 16 VA. L. WEEKLY DICTA COMP. 31, 33 (1965).

[31] Zemel v. Rusk, 381 U.S. 1, 17 (1965).

privacy as opposed to the diverse importance of substantive goals toward which various privacy-invading investigations lead. While the balances will surely be struck differently in different investigatory contexts, it would make no sense to approach each case as if the decision were to be written on a clean slate. The investigative system demands guidance for its millions upon millions of information exchanges each year. What is needed is the creation of some broad rules to govern large classes of cases. By analogy to the statutes that designate some government records as public and others as confidential, the legal system can afford some individual-case sacrifices of either the values related to privacy or those related to a free information flow in order to achieve a workable accommodation of those values in the great, regularized majority of cases. The latter portions of this article are principally addressed to the creation of such broad substantive rules for two important problem areas, within the framework for analysis here suggested.

Before leaving the subject of unjustified access to personal data, however, we should devote some attention to the kinds of remedial measures that might be proposed.[32] In our typical case, the traditional civil remedies of damages, restitution, and injunction all leave a great deal to be desired. Even in classic invasion of privacy cases, involving publication in the mass media, "it has not proved possible to measure damages for [the tort],"[33] and verdicts tend to run low, well below those for defamation.[34] When the publication of information out of a personal data file is made only to a few interested persons, not only must we stretch the substantive definitions of the tort;[35] we must also be prepared to justify giving money damages to compensate the subject for the disclosure. How is he harmed by the communication of the truth? (I leave the discussion of false statements to the section on accuracy.[36]) If he is, for example, denied a job, is not the prospective employer correspondingly benefited by being apprised of the information that causes him to refuse to employ the subject? If the courts, in the face of that justification, should nonetheless find an unreasonable (tortious) disclosure, it is legitimate to suggest that the same justification still deserves consideration in the determination of damages.[37]

[32] Criminal penalties are, of course, one possible solution. It is a crime, for example, for employees of the Internal Revenue Service to divulge information from federal income tax returns unless the disclosure is authorized by law. INT. REV. CODE OF 1954, § 7213(a)(2) provides a punishment of a year's imprisonment or a fine of $1,000, or both. VANCE PACKARD, THE NAKED SOCIETY 192 (1964) says that the going price for an illegal view of a return is a minimum of $1,000. While the identity of the fine and the "fee" is no doubt fortuitous, it is possible that such disclosures are expensive because of the fear of prosecution. An alternative explanation that seems more likely is the fear of *detection* and dismissal. Serious criminal penalties in this area are heavy artillery used against insects.

[33] Kalven, *The Right of Privacy Under the Shadow of the Constitution*, in THE RIGHT OF PRIVACY, 16 VA. L. WEEKLY DICTA COMP. 76 (1965). See also Kalven, *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, *supra*, pp. 326-41, especially p. 334; Note, *Recent Developments in the Right of Privacy*, 15 U. CHI. L. REV. 926, 932-36 (1948).

[34] See Franklin, *A Constitutional Problem in Privacy Protection: Legal Inhibitions on Reporting of Fact*, 16 STAN. L. REV. 107, 141 (1963).

[35] See text at notes 18-20 *supra*.

[36] See text accompanying notes 57-84 *infra*.

[37] Professor Franklin makes a similar point by analogy to "the instinctive distinction between coerced

In any case, damages are so unlikely to be substantial that the typical lawsuit will not be worth the trouble, and the threat of damages will be a flimsy deterrent to unjustified disclosures.

Restitution in any literal sense is simply impossible in the context of disclosures of sensitive data; once made, a disclosure cannot be erased.[38] And while some efforts have been made to use an unjust enrichment theory to pursue the profits from mass-media privacy invasions, such as book royalties, those efforts have not succeeded.[39] Furthermore, the amount of profit made by an investigator from any single disclosure of personal data will almost always be so small as to discourage the victimized subject from suing.

The traditional rule forbidding injunctions against libel has by no means been followed consistently in privacy cases.[40] There are, however, serious constitutional doubts about the validity of an injunction against the disclosure of information not shown to be false. *Near v. Minnesota*[41] and its progeny,[42] reinforced by the recent decision in *Garrison v. Louisiana*,[43] discussed below, will probably present an insuperable obstacle to such injunctions in the future. Most of the modern cases sustaining injunctions against privacy invasions have been based on either the plaintiff's quasi-proprietary interest in the commercial exploitation of his own personality[44] or his interest in avoiding being publicized in what Dean Prosser calls a "false light."[45] Those decisions do not support an assumption that injunctive relief will be generally available against the wrongful disclosure of sensitive personal information that is true; the opposite proposition would be a safer prediction.

Even so, constitutional doctrine is not the most formidable hurdle for injunctive relief to surmount in cases of improper access to sensitive files. Dwarfing all doctrinal issues here is the difficulty of finding out about the disclosure. Discovery of the wrongdoing is, of course, a prerequisite to any remedial action, and discovery is peculiarly difficult when the wrongful disclosure has been made in aid of a "con-

confessions [which may be false] and [the fruits of] illegal search and seizure" in the pre-*Mapp* era. Franklin, *supra* note 34, at 141 n.140.

[38] Of course, further disclosure can be limited by erasure. See the discussion of California's legislation authorizing the "sealing" of some criminal and juvenile records in text accompanying notes 122-35 *infra*.

[39] *E.g.*, Hart v. E. P. Dutton & Co., 197 Misc. 274, 93 N.Y.S.2d 871 (1949), *aff'd mem.*, 277 App. Div. 935, 98 N.Y.S.2d 773 (4th Dep't 1950); Cason v. Baskin, 155 Fla. 198, 20 So.2d 243 (1945).

[40] See Note, 15 U. CHI. L. REV. 926, 932 (1948). The classic criticism of the rule against enjoining libels is Pound, *Equitable Relief Against Defamation and Injuries to Personality*, 29 HARV. L. REV. 640 (1916).

[41] 283 U.S. 697 (1931).

[42] While prior restraints on speech are not necessarily unconstitutional under all circumstances, recent decisions of the Supreme Court make clear that prior restraints are constitutionally suspect, requiring a demonstration that they avoid the principal evils of censorship. *E.g.*, Freedman v. Maryland, 380 U.S. 51 (1965).

[43] 379 U.S. 64 (1964). See discussion in text accompanying notes 46-56 *infra*.

[44] *E.g.*, Haelan Labs. v. Topps Chewing Gum, Inc., 202 F.2d 866 (2d Cir. 1953).

[45] This is the explanation of the decisions enjoining the retention of innocent persons' photographs in rogues' galleries. See Note, 15 U. CHI. L. REV. 926, 927 n.7 (1948). *But cf.* Brex v. Smith, 104 N.J. Eq. 386, 146 Atl. 34 (Ch. 1929) (injunction granted against a public official's investigation of individual bank accounts of members of police force).

fidential" investigation. Those difficulties are compounded and quite beyond the reach of the legal system when the discovery must be made sufficiently in advance of the impending disclosure to secure judicial action.

Any discussion of judicial remedies against wrongful access to personal data must come to terms with the still-uncertain reach of first amendment protections of truth. The holding of *Garrison v. Louisiana*[46] can be stated narrowly: truth alone, without any additional requirement of good motive, must be a defense to a prosecution for criminal libel when the alleged libel was directed against a public official's conduct of his public duties. Since the Supreme Court relied so heavily on *New York Times Co. v. Sullivan*,[47] however, it is as certain as any doctrinal statement can be that a similar limitation would be placed on the award of damages in civil libel actions arising in any of the few states that place "good motive" limits on the defense of truth.[48] The starting point for analysis is thus a principle that truth is a constitutional defense to libel of a public nature.[49] Our task is to estimate how that principle may come to affect efforts to afford judicial protection against the wrongful disclosure of personal data.

Mr. Justice Brennan's opinion for the Court expressly limited its holding to libels relating to public affairs, in this significant footnote:

> We recognize that different interests may be involved where purely private libels, totally unrelated to public affairs, are concerned; therefore, nothing we say today is to be taken as intimating any views as to the impact of the constitutional guarantees in the discrete area of purely private libels.[50]

Equally significant, the opinion noted Lord Campbell's old rejection of the idea that "a man's forgotten misconduct, or the misconduct of a relation, in which the public had no interest, should be wantonly raked up, and published to the world, on the ground of its being true."[51] That concern was not present here, said Mr. Justice Brennan, because here the public is vitally interested in the conduct of its officials, so that "the interest in private reputation is overborne by the larger public interest, secured by the Constitution, in the dissemination of truth."[52] Finally, another footnote speaks approvingly of the newsworthiness limitation in actions for invasion of

[46] 379 U.S. 64 (1964).

[47] 376 U.S. 254 (1964).

[48] See Franklin, *The Origins and Constitutionality of Limitations on Truth as a Defense in Tort Law*, 16 STAN. L. REV. 789, 835-48 (1964).

[49] The Supreme Court has just begun to explore the boundaries of the concept of public speech. See Rosenblatt v. Baer, 383 U.S. 75 (1966). See also HARRY KALVEN, JR., THE NEGRO AND THE FIRST AMENDMENT ch. I (1965); Kalven, *The New York Times Case: A Note on the Central Meaning of the First Amendment*, 1964 SUP. CT. REV. 191; Karst, *The First Amendment and Harry Kalven: An Appreciative Comment on the Advantages of Thinking Small*, 13 U.C.L.A.L. REV. 1 (1965).

[50] 379 U.S. at 72 n.8. "Private" libels may perhaps be repressed, not because they are more damaging to the individual victims' reputations, but because their repression results in less damage to the governing process. See Karst, *supra* note 49, at 12 n.53.

[51] 379 U.S. at 72.

[52] 379 U.S. at 73.

privacy, thus at least arguably accepting by implication the constitutionality of an award of damages in a privacy case in which the publication cannot be shown to be newsworthy.[53]

This language suggests that *Garrison* will not be extended to limit a state's power to impose sanctions against the kind of improper disclosure with which we are concerned. But our situation, like that in *Garrison*, differs from the case that Lord Campbell feared. The wrongful publication of information from personal data files usually is not made "to the world" but to a limited, typically small, number of recipients.[54] The recipients, furthermore, will have as much "interest" in receiving the information as the public normally has in learning about its officials, at least in the descriptive sense of the word "interest."[55] If Lord Campbell was speaking of what the public ought to be concerned with, we have been carried back to the "need to know" dilemma,[56] and our remedial issues begin to resemble the substantive questions about the propriety of access. Whether or not the *Garrison* case portends a general tightening of constitutional standards in the area of damages for invasion of privacy, its strong statement of "the public interest . . . in the dissemination of truth" should not be ignored by state courts faced with similar problems at a non-constitutional level. At the very least, *Garrison* reinforces the dual requirement in common law damage actions that "private facts" be made "public."

The poverty of traditional remedies suggests that other controls over the custodians of personal data files may be more appropriate. Since the merits of proposals for other kinds of control—such as administrative discipline of governmental custodians and professional licensing or bonding of private custodians—are so closely bound to the operational needs of each information storage system, their discussion is reserved for the latter sections of this article.

B. Accuracy

The pessimism expressed in the foregoing discussion of possible limitations on access to personal data springs from doubts about both their substantive and their remedial viability. Efforts to improve the accuracy of the files, however, are another matter. Here the interest in the free flow of information is only marginally involved, and the chief remedial concern in several important classes of cases is that corrective systems may be costly.

Inaccuracy of the simplest kind, such as the case of mistaken identity, is conceptually the easiest to deal with. Once such a clear-cut mistake is discovered and called to the attention of the proper authority,[57] it is to be expected that the file will

[53] 379 U.S. at 73 n.9.

[54] And therefore not actionable as the common law now stands. See text accompanying note 20 *supra*. This constitutional discussion is thus in the "What if . . . ?" category.

[55] *Cf.* Note, *The Right of Privacy: Normative-Descriptive Confusion in the Defense of Newsworthiness*, 30 U. CHI. L. REV. 722 (1963).

[56] See text accompanying notes 13-31 *supra*.

[57] There may be an additional problem in finding someone who considers himself to be the proper authority.

be corrected. The most serious problem raised by inaccuracy of this type is that of discovering it.[58] There are, however, other kinds of inaccuracy that are somewhat harder to define, and much harder to remedy; these are the half-truth and the evaluative statement.

Of course every statement is a half-truth, in the sense that it does not explain everything. No one suggests that every personal data file must begin with the cosmos. In deciding whether a record is complete, telling "the whole story," we need to know the purposes behind the record's compilation and use. A statement may be adequate for some recipients but misleading when passed on to others without explanation. A man who tells his draft board that he has been divorced, for example, feels no need to add that his former wife has remarried. The same bare, unexplained statement, passed on to a credit investigation file, might be an obstacle to the subject's obtaining credit until the file is made to show that he has no obligation to pay alimony.

It may be objected that the case just stated presents a problem in access, not accuracy; the appropriate remedy would be to keep the credit investigators out of the draft board's records. While there is some doubt of the feasibility of such a direct limitation, it is doubtful in the extreme that any system of statutory or administrative limitations can prevent the information from getting to the credit man indirectly, through other public and private investigative middlemen, all of whom can demonstrate at least an arguable "need to know." The sequence of (1) draft board, to (2) police department, to (3) industrial security investigator, to (4) employment file, to (5) credit investigator is not an unrealistic example.[59]

The access and accuracy problems are complementary: we worry about widespread access partly because we doubt the accuracy of the information passed along from one file to another, and we worry about accuracy partly because we fear that efforts to limit access will fail. California's legislation authorizing the "sealing" of certain criminal records, discussed below,[60] may be thought of as a limitation on access to the facts about the subject's isolated youthful indiscretion. But we limit access because we assume that statement of the early conviction, although true enough, is misleading; it is a half-truth, for its fails to disclose the subject's later rehabilitation. For some purposes, presumably the statement would not be significantly misleading. The fact of the conviction and resulting detention may even provide the subject with an alibi or with an excuse for not being somewhere else at the same time. We sacrifice some "legitimate"—nonmisleading—relays of the information because we think the information will mislead in too many cases. We are once more faced with the difficult task of evaluating claims of relevancy: Is it *proper* for a prospective employer to consider the fact that the subject stole a car when he was fifteen? Should the law

[58] See the remedial discussion in the text accompanying notes 77-83 *infra*.

[59] The distortion of half-truths is aggravated to the extent that there is pressure on investigators to produce derogatory data. See MYRON BRENTON, THE PRIVACY INVADERS 14, 36 (1964).

[60] See text accompanying notes 121-35 *infra*.

decide in advance on the employer's behalf that he would be misled if he were allowed to learn of the juvenile court record?

The existing tort law of privacy recognizes the problem of the half-truth in decisions permitting recovery when the defendant publishes material that places the plaintiff in a "false light," even though what is published is literally true. When Al Ettore unsuccessfully fought Joe Louis, he fought a relatively good third round. When the films were later shown on television, the third round came to rest on the cutting room floor, and the viewing public saw only those portions of the bout that showed Ettore less favorably. The resulting lawsuit[61] was decided against Ettore; the judges of the Third Circuit viewed the films, and concluded that "the omissions were *de minimis*."[62] The theory of recovery, however, "might have afforded a cause of action to Ettore,"[63] if his third round had impressed the judicial fistic critics more. The *Ettore* dictum reflects numerous holdings in other similar cases: a perfectly accurate photograph is published with a misleading caption;[64] an innocent man's photographs or fingerprints are kept in a "criminal" file.[65]

As personal data files become more centralized and more accessible, they will also become more complete.[66] The more complete the files are, the more likely we are to assume that they contain full profiles of their subjects. The problem of Al Ettore's good third round takes on a more serious aspect in the context of a security investigation based on a trusted but incomplete file.

Assuring that the file contains "the whole story" is not always easy at present. In the first place, the subject typically will not know of the significant omission; very often, he will not even know that the file exists. And if we make the big assumption that he is given access to his own file, there are staggering conceptual problems in devising an objective standard for defining the outer boundaries of one "whole" truth. Some investigative agencies, recognizing this difficulty, make it a practice to interview the subjects of their investigations. They reason that the subject himself will often be glad to have a chance to reply to derogatory information in the investigator's possession and that in doing so he will improve the reliability of the file. A private agency which sells its investigative services lives by its reputation for reliability, and has a substantial interest in getting the whole story. May there

[61] "Ettore apparently, at first at least, did not object to the telecasts, despite the fact that he was not compensated therefor; for he informed his friends that they should watch for the third round. Only after he had discovered that the third round had been omitted did he claim damages to his rights of privacy and property." Ettore v. Philco Television Broadcasting Corp., 229 F.2d 481, 483-84 n.4 (3d Cir. 1956).

[62] *Id.* at 496.

[63] *Id.* at 495.

[64] *Compare* Gill v. Hearst Pub. Co., 40 Cal. 2d 224, 253 P.2d 441 (1953), *with* Gill v. Curtis Pub. Co., 38 Cal. 2d 273, 239 P.2d 630 (1952) (same photograph, accurately captioned in one article but misleadingly captioned in another; liability in the latter case).

[65] Photographs tend to raise more privacy problems than do fingerprints, since only an expert can make anything out of a set of fingerprints. See Note, 15 U. CHI. L. REV. 926, 927 n.7 (1948).

[66] See text accompanying notes 84-104 *infra*, on the role of the computer.

not be a legislative lesson in this practice? The discussion of remedies against inaccuracy at the end of this section proposes to give the initiative for such efforts at amplification to the subjects of certain kinds of files.

Just as every truth is a partial truth, every statement of fact is at least partly an evaluation. The courts' abiding inability to separate "fact" from "opinion"[67] is inherent in the use of language to represent things. Even the statement that the subject of the file is thirty years old implies some evaluation: either he is between his thirtieth and thirty-first birthdays, or he is nearer to his thirtieth birthday than to another. That degree of evaluative content, however, is tolerable most of the time; the recipient who knows that he needs more precision will make further inquiry. But a statement in an insurance investigation file that classes the subject as a "spree drinker," or as a "class 4C" drinker, is tolerable or not, depending on the use that is made of the statement. And what is more conclusory than the notation in a security investigation file, "cited by HUAC"?

An evaluative statement may appear in a personal data file, such as an employment file that includes rating sheets prepared by the subject's supervisors. Or the evaluation may be made from relatively factual statements in the file by its custodian or by an investigator who gains access to it. A former private industrial security investigator, who had previously been a law enforcement officer for many years, told me that during his investigative career he had experienced no difficulty in obtaining information from law enforcement files but that he never turned derogatory information over to his clients. Instead, he just told them that a prospective employee was not suitable. In those circumstances, as in the case in which the foreman gives a subordinate a "C" rating for his industry, or his ability to get along with co-workers, there are substantial risks of misunderstanding.

Any description or evaluation involves a selection, conscious or not, by the evaluator of one significant characteristic or a group of them, out of a great many, followed by a generalization based on the selected traits. This basic reasoning process will be familiar to any lawyer.[68] There is nothing wrong with the process of abstraction and generalization; indeed, it is inescapable. The danger of inaccuracy lies in the fact that the evaluator and the recipient of his statement may not share the same standards for reducing a complex set of facts to evaluative inferences[69] or even the same language. Those risks are minimized within an institution whose members share common training and traditions. Every commissioned officer in the armed forces knows, for example, that what appears to be a middle-range effectiveness rating is really a low rating; the subject's present commander will not be misled by

[67] Similar difficulties are present in the criminal law of false pretenses and in the tort law of defamation, business disparagement, and misrepresentation.

[68] See EDWARD H. LEVI, AN INTRODUCTION TO LEGAL REASONING (1949).

[69] These words are written just at the close of the semi-annual season for grading examinations.

a former commander's rating.[70] The risk of inaccuracy is greatest when the file is read by an outsider who is not familiar with the system and who is not aware that the language or the standards of the evaluator differ from his own. Here is another overlap with the problem of improper access; when access to a file is limited to the group for which it was prepared, the risks of misunderstanding decrease.

In some areas of present tort law, the law gives the appearance of having been designed to encourage the use of slippery, evaluative words. In the business disparagement case of *Mayfair Farms, Inc. v. Socony Mobil Oil Co.*,[71] two restaurant owners sued the publishers of the *Mobil Travel Guide*, a book which rated hotels, motels, and restaurants. One of the restaurants had been given a one-star rating, and the other a two-star rating. Both complained that they should have been given higher ratings (the highest possible is five stars), and sought an injunction against distribution of the guide in its existing form. The New Jersey judge denied the relief, concluding "that the differences between the parties are basically differences of judgment or opinion."[72] So long as the evaluator keeps his statements fuzzy and evaluative, he is in little danger. Much the same can be said of the remnants of the "fair comment" area of defamation privileges,[73] although *New York Times Co. v. Sullivan*[74] makes the fact-opinion distinction unimportant in cases of defamation of public officials.[75]

Even without the law's encouragement, however, most statements about our fellow men can be expected to include elements of evaluation and criticism that go beyond the facts, narrowly conceived. Personal data files, far from being an exception to the rule, will continue to demonstrate it. There is a market demand for evaluation. Of course the files will vary in their relative emphasis on "fact" and "opinion," with those generated by investigative agencies tending most strongly toward evaluation.[76] It is ironic that the very files which are least likely to contain half-truths—those produced by investigative leg-work—are the most likely to contain evaluative gossip and rumor, while the files which tend to avoid evaluation—typically, those maintained by noninvestigative public offices and open to the public—are more apt to mislead because they do not tell enough. While clearly mistaken information is normally corrected upon discovery, and therefore relatively scarce, these more subtle forms of inaccuracy feed on themselves.

[70] I have it from my colleague, Professor Benjamin Aaron, that when a civil servant receives a rating below "excellent" the rating is often the subject of a complaint.

[71] 68 N.J. Super. 188, 172 A.2d 26 (Sup. Ct. 1961).

[72] *Id.* at 192, 172 A.2d at 28. The court was also reluctant to enjoin the distribution of the book, on traditional free speech grounds.

[73] See, *e.g.*, the savage criticism of a vaudeville act, preserved for posterity in the court's opinion in Cherry v. Des Moines Leader, 114 Iowa 298, 86 N.W. 323 (1901).

[74] 376 U.S. 254 (1964).

[75] And, perhaps, other types of "public speech" as well. See note 49 *supra*.

[76] This criticism cannot be attached to the work of the old established business reporting firms, which regularly give the subjects of their investigations an opportunity to clear up any apparently derogatory information.

The remedy, once an inaccuracy is authoritatively identified, is of course to subtract from the file, to add to it, or to do both. Precedent is available for subtracting, in legislation permitting the sealing of criminal or juvenile records[77] or even the return to an accused person of photographs and fingerprints in his police file in the event of an acquittal.[78] Parallel authority exists within the armed services for "correction" of a military record, even in some cases in which the correction amounts to a rewriting of admitted historical fact.[79] The right to add material to one's personal data file finds general precedent in the fundamental principle of the adversary system which permits criminal and civil defendants to introduce testimony favorable to them. More particularly, such a precedent may be found in a "right of reply" to mass-media defamation[80] and in laws and regulations that permit government employees to comment upon unfavorable ratings given them by their superiors.[81]

It is easy to say what should be done when an inaccuracy is *authoritatively* identified. The more difficult questions relate to the manner in which such an authoritative conclusion can be reached in cases of resistance by the custodian of the record. First, the subject of the file, or someone acting in his interest, must discover the asserted inaccuracy. Second, he must find a court, or some other authority, that is empowered to order the record's correction. And, third, he must be able to establish the inaccuracy to the satisfaction of the authority. The latter requirement need not be examined here, although there are some aggravations of the usual problems of proof associated with personal data files—notably the stale evidence problem and the difficulty of proving that an unfavorable evaluative statement is false. The first two requirements, however, are critical.

Discovery of the inaccuracy depends on the subject's access to his own file and his awareness of the need to inspect it. Even when a record is freely accessible to its subject, there is no assurance that the subject will know of its existence or its contents. Any system of routine notification of additions to personal data files will be resisted on grounds of cost, and with reason; mailing costs alone would be enormous. What may be more feasible is the identification of certain files or certain types of information as worthy of the expense of notice to the subject.

In any case, notice to the subjects of the files is not their most serious need, as a class; a legislator dedicated to improving the accuracy of certain kinds of personal data files would instead begin by granting their subjects a right of access to them. Such a right even takes precedence over giving the subjects a tribunal with the power to correct the files, for often the custodians themselves will be willing to make correc-

[77] Discussed in text accompanying notes 122-35 *infra*.

[78] N.Y. PEN. LAW § 516.

[79] The basic legislation is 10 U.S.C. §§ 1551-54 (1964).

[80] See 1 ZECHARIAH CHAFEE, GOVERNMENT AND MASS COMMUNICATIONS 145-95 (1947); Donnelly, *Right of Reply: An Alternative to an Action for Libel*, 34 VA. L. REV. 867 (1948).

[81] *E.g.*, 64 Stat. 1099 (1950), 5 U.S.C. § 2006 (1964).

tions that are shown to be justified. What will be objected to by custodians as a class is the cost of a system of access. Furthermore, both public and private investigative agencies will be concerned over the possibility of compromising sources of information. If the rather mild requirements of the case of *Jencks v. United States*[82] horrified the leadership of the FBI,[83] one can imagine the reaction of law enforcement officials to a statute giving anyone the right to demand access to his police files.

The cost of a system of access can be reduced radically by limiting access to the occasions of certain critical events: the refusal of employment, or credit, or insurance. Further reductions of cost might be achieved by limiting the number of inspections during specified periods. If automation will significantly reduce the costs of access to investigators, it will do so to the same extent for the subjects themselves.

Compromising of investigative leads or the identity of informants need not result from a system that allows some limited inspection of the records of investigative agencies. One can imagine, for example, legislation specifying that access must be given to some types of information but not to others. The result would surely be the keeping of two sets of files by such agencies, but that practice would not defeat the goals of the legislation. The subject would be given a chance to clear up the plain mistakes, to his and the agency's mutual advantage. Furthermore, the creation of two sets of files would encourage more restrictive security practices with respect to the more sensitive files, while granting relatively free access to the more routine information. The latter practice would be a departure from the form, but not the substance, of present procedure.

There is no logical or practical difficulty in establishing judicial or administrative authority to order the correction of a personal data file upon the petition of the subject. There is, however, an important difference between granting that body the power to order an addition to a file and giving it the power to erase. There are values of a constitutional dimension that are compromised by any attempt on the part of government to erase records of historical data that are true. One who consciously lies in rewriting history bears a weighty burden of justification; it will be recalled that Orwell's all-knowing state did so for perfectly benevolent reasons. While such considerations may not make "expungement" legislation unconstitutional, they deserve serious consideration in striking the legislative balance.

C. The Computer: "Just as Long as They Spell Your Number Right . . . ."[84]

The automation of data processing can no longer be regarded as a costly frill. It is a present necessity if we are to avoid "disappearing beneath an avalanche of tons

[82] 353 U.S. 657 (1957).

[83] FRED J. COOK, THE FBI NOBODY KNOWS 382-90 (1964); *cf.* DON WHITEHEAD, THE FBI STORY 287-90 (1956).

[84] In this section I have drawn heavily on these papers: ELDRIDGE ADAMS, COMPUTERIZATION OF THE LEGAL SYSTEM: THE NATURE OF THE REVOLUTION (1964); ELDRIDGE ADAMS, ELECTRONIC DATA PROCESSING

of red tape, paperwork and filing cabinets."[85] Correspondingly, it will result in a net saving in the cost of processing information. In short, personal data files, like others, are right now being transferred from filing cabinets to computer tapes,[86] with significant implications for both the access and accuracy aspects of our analysis.

In relation to present systems, the computer will permit the collection and storage of more detailed data, its collation in more meaningful form, and speedier access to stored data. Because an investigator with access to the computer need not go to the original sources of information, his investigation can be made at substantially reduced "cost-per-unit-dirt,"[87] if that is not too emotion-charged a term. In almost any other context, the encouragment of inquiry by reducing its cost is universally applauded. And while our generation inclines toward making at least a visceral exception for personal data, it is doubtful that our children will feel the same way.[88]

A computer is an expensive instrument and needs to be used fully to justify its cost. The result is that a number of users may come to share the time of a single computer, just as a number of conversations are carried simultaneously over one cable.[89] Not only the computer's time but also its stored information can be shared. The fact that one investigator seeks access to another's files demonstrates that needs for the same information overlap, and there is a resulting economic pressure on various users to pool their data in centralized storage. Government agencies are taking the lead in data sharing,[90] but private organizations will not be far behind.[91]

The risks of leakage in a shared-time system are obvious. One user may interrogate another's files accidentally—or deliberately if he knows the password. Furthermore, while in theory centralization of data storage permits closer control over

---

AID TO THE COURTS (1964); PAUL BARAN, COMMUNICATIONS, COMPUTERS AND PEOPLE (1965); Michael, *Speculations on the Relation of the Computer to Individual Freedom and the Right to Privacy*, 33 GEO. WASH. L. REV. 270 (1964).

[85] *Brown Asks Electronic Data Link-up*, Los Angeles Times, Feb. 21, 1966, pt. III, p. 7, col. 8.

[86] The transfer is beginning with routine, standardized information. Highly individualized investigative reports are more difficult for computers to manage, and yet their storage is well within the capacity of present technology.

[87] This is Dr. Baran's phrase. BARAN, *op. cit. supra* note 84, at 12.

[88] See Fadiman, *Please Tap My Wire, I Like It!*, Holiday Magazine, July 1964, p. 12.

[89] Time sharing among various businesses is well under way. See *Sharing the Computer's Time*, Time Magazine, Nov. 12, 1965, p. 104, col. 3.

[90] See *Use of Electronic Data Processing Equipment in the Federal Government*, H.R. REP. No. 858, 88th Cong., 1st Sess. 9 (1963): "As a part of the electronic data processing systems standardization program, work on machine-to-machine reporting (data interchange) should be intensified." See also *Brown Asks Electronic Data Link-up, supra* note 85; *Center for Data on Everybody Recommended*, Washington Post, June 13, 1966, p. A3, col. 1 (reporting on a recommendation of a consultant to the Bureau of the Budget).

[91] One leading prospect for transfer of personal data to a national computerized system is the existing compilation of insurance investigation data. Vance Packard reports that computers are already selecting policyholders for spot-check "special" investigations. THE NAKED SOCIETY 142 (1964). "The 'Index System' is a clearinghouse for personal injury claims records; in 1962, it had 16,704,266 claims on file. The Casualty Index, manned by the Hooper-Holmes Bureau, serves some 110 accident and health companies and has accumulated more than 6,500,000 claims files." MYRON BRENTON, THE PRIVACY INVADERS 51 (1964).

access to the data,[92] the necessity of speedy national distribution of the data to authorized recipients requires that access be made available to persons at many locations remote from the central data bank. At present the data are transmitted over the telephone lines and microwave relay system of the national communications network. An investigator who knows the right passwords can tap a computer just as surely as he can tap a telephone wire.[93]

Finally, the computer will influence our choices as to the access problem by widening our concepts of relevancy. As we learn to use computers to build progressively refined predictive models of human behavior,[94] more and more information will be useful to the predicting agencies. All sorts of data hitherto considered to be nobody else's business will turn out to have great relevance for decision-making about the subject of the electronic data file. Part of the reason that some data are now regarded as private, or intimate, is that their utility in the predictive process is not discernible. When the behavioral scientists are able to prove their utility, we will probably change our minds about limitations on access.

The computer's contributions to the accuracy problem should be for the most part benign. There are, however, some subtle dangers. The sharing of information in a unified storage system implies a standard classification scheme. One result will be that, although the various users of the data may have different purposes, they will have to accept a common language, at least at one stage of the processing.[95] At first, we can foresee a loss in accuracy and understanding, for some of the users will be unfamiliar with the terms of the common language. Later, as new generations of users grow up with the same terms, perhaps this kind of misunderstanding will tend to disappear. Perhaps; or will the use of the same language simply be deceptive, creating a language barrier like the one which is the source of so many jokes about Americans in England? This latter kind of misunderstanding may be tolerable just because it takes place on a sophisticated level.

Another effect of a centralized, standardized data processing system is that the facts that emerge from the computer will become the only significant facts about the subject of the inquiry. This tendency is inherent in any system of data storage, including a manila folder; it is simply intensified by use of the computer, because of the very great differences, in convenience and cost, between accepting what the computer tells us and going behind its report to the original sources of information. So it will be harder to fill in the gaps, the half-truths. And when the subject himself tries to explain, he will be met with more resistance precisely because he has to rely on

[92] Rowan, *Cybernation and Society: An Overview*, SDC Magazine, Sept. 1965, p. 1.

[93] BARAN, *op. cit. supra* note 84, at 13.

[94] See Michael, *supra* note 84, at 283; Ruebhausen & Brim, *supra* note 6, at 1196-98.

[95] Of course, the computer is capable of changing the form of expression of either input or output, so that users will not necessarily have to speak to it in the same language. However, if data are to be exchanged, at one point in the processing system they must be reduced to a standardized form of expression. See H.R. REP. No. 858, 88th Cong., 1st Sess. 9, 46-48 (1963), for a discussion of EDP standardization within the federal government.

outside sources, which are apt to be thought of as softer, lacking the computer's deceptive precision.[96]

The making of evaluative statements on the basis of raw data may, in great measure, be turned over to the computer. The same kind of technology that permits computers to diagnose heart disease will permit them to evaluate antisocial tendencies or credit risks. Indeed, it is presently within our capability to construct a fully automated retail credit system in which the saleslady inserts the customer's card into a slot and is told by a nationwide computer network in a matter of seconds whether, or how much, credit will be allowed by the customer's lender.[97] While mechanized evaluations of that kind plainly will be useful as an adjunct to other evaluations which take into account individual peculiarities, the chances are good that in a number of contexts the more "personalized" evaluations will not be supplemented but replaced. A credit manager who prides himself on making an individual decision on each applicant may be forced to sacrifice much of that personal attention in order to take advantage of the substantial cost savings that can be achieved by full reliance on the computer's evaluation. And while he may be quite conscious of what he is giving up, another investigator who sees only the final print-out may be deceived into attributing more to the computer's evaluation than it deserves. In the world of automated processing of personal data, too, issues of access and accuracy blur together.

An even more disturbing illustration of the latter point is the power of a malevolent computer-tapper to alter the contents of a personal data file. Not only may our bad-man-with-the-password find out what is in the data bank; he can make his own deposits and withdrawals, all in someone else's name, by erasing or adding information so as to create a false record for the subject of the file. Furthermore, we must expect some programmers who have regular access to personal data files to be subject to bribery or other improper persuasion. Not only will such persons have the power to grant access to the wrong people; they will also have the power to "invent a private life"[98] by their selection and arrangement of the information to be retrieved from the computer.

Two remedial devices that might respond to the special challenge of computerized personal data systems are the professionalization of at least some high-level programmers and regulation of the manufacture and use of the systems' equipment. The word "professionalization" is chosen deliberately to suggest something beyond a licensing scheme. Licensing alone is inadequate; private investigators are required to be licensed in many states;[99] enough said. Rather what is envisioned is a body of "certified public programmers," with disciplinary powers over its own members

[96] Michael, *supra* note 84, perceptively analyzes these problems in psychology.

[97] See text accompanying note 155 *infra*. To assure that persons other than the customer do not interrogate the computer about his credit standing may require the customer to submit to other invasions of privacy which are implicit in a nearly foolproof identification system.

[98] Michael, *supra* note 84, at 280.

[99] *E.g.*, CAL. BUS. & PROF. CODE §§ 7520-7543.

similar to those exercised by existing professional bodies.[100] Past efforts to draw up an ethical code for "computer people" have resulted in rather cloudy statements of concern over what might generically be called "the Oppenheimer problem": Suppose you are a computer man working for a government which orders you to build a computerized doomsday machine, etc.[101] That is not the kind of ethical standard with which we are concerned here. A more modest and more attainable goal might be the establishment of a set of principles to govern confidential relationships, drawing on the experience of the medical and legal professions.

Regulation of those who manufacture or lease data processing equipment will not be popular with computer men,

> as it carries with it a built-in loss of freedom. The thought of the creation of another governmental agency peering over one's shoulder contains the seeds of the possibility of bureaucratic decay and arbitrary conclusions based upon an incomplete understanding of complex problems . . . . The extreme competence that we need in a regulatory agency of this type is too rare a commodity.[102]

But Dr. Baran himself, the author of those warning words, has given us a set of minimum safeguards that might serve as a beginning: The use of simple cryptography, double password systems to avoid accidental "dumping" of sensitive data, audits of programmers to avoid "backdoor" entry, mechanisms to detect unusual interrogations of the computer, recording of the sources of interrogations[103]—all of these goals are understandable by laymen, even when the precise mechanics for achieving them are not. One need not be a nuclear physicist to be a member of the Atomic Energy Commission. A company that leases time on the same computer to several customers can be thought of as occupying a position analogous to that of a public utility. When the service of such a company is the processing of sensitive personal data, it does not seem overly burdensome to insist that certain minimum security procedures be followed. No one suggests that banks in Switzerland are about to founder because the government requires them to keep confidential the names of their numbered-account depositors.[104]

II

TWO TENTATIVE APPLICATIONS

While the same kinds of questions need to be asked about accuracy and disclosure in a wide variety of factual contexts, the various institutional answers are sure

[100] It is important to remember that the word "programmer" describes a wide variety of levels of occupation. Some programming tasks are roughly comparable in level of sophistication to bookkeeping, as distinguished from accounting. It is only the more highly trained programmers, or those performing the most sophisticated work, who should be considered for professionalization.

[101] *The Social Responsibilities of Computer People* (Report to the Council of the Association for Computer Machinery by the Committee on the Social Responsibilities of Computer People, presented Dec. 1958), in EDMUND C. BERKELEY, THE COMPUTER REVOLUTION 220 (1962).

[102] BARAN, *op. cit. supra* note 84, at 14-15.

[103] *Id.* at 16-17.

[104] See Fehrenbach, *Secrets of the Swiss Banks*, The Atlantic, July 1965, p. 33.

to diverge. The predictable differences in public response to the various alleged privacy invasions and other abuses of personal data collections are not primarily related to any such differences as there may be in the degree to which the interests of the file subjects are adversely affected. Instead, it may be guessed that legislative and other governmental policy in this area will come to be influenced chiefly by public attitudes toward the value of each investigative or data-collecting agency. What becomes of the files of the House Committee on Un-American Activities, for example,[105] is very likely to be determined by the degree of public support that can be marshalled for the Committee's work in general. The reason is not simply that the files are closely related to the Committee's main function of exposure[106] but, more fundamentally, that it is hard to get either the public or its representatives to think in any but the grossest terms about such problems. The very narrow discovery rule of the *Jencks* decision seemingly was taken by so knowledgeable a citizen as Director Hoover as a frontal attack on the FBI, judging from his vigorous response; it is no surprise that it came to be widely assumed that the decision had "opened the FBI files."[107]

Beyond that mild despair about the black-and-white world of politics, there is a deeper difficulty that inheres in our subject matter. I have tried to demonstrate in Part I of this article that it is not possible to separate an analysis of legislative or other policy needs relating to access to personal data, or to controls over its accuracy, from one's views about the utility of the various operations that produce and use the data. Therein lies my first warning about the discussions that follow. The reader who does not share the values implicit in this discussion is invited to substitute his own, within the relatively objective framework of Part I.

My second warning is in the nature of a disclaimer of expert competence. The applications that follow are tentative, as the title of this part emphasizes, because I have no special qualifications, beyond that of an interested citizen, to evaluate the internal operations of either police departments or credit bureaus. Those agencies have been selected for closer attention in order to show how the general analysis of Part I might be applied in some particular situations and because it seemed appropri-

[105] It is often asserted that the HUAC files list a million names. Access to the Committee's raw files is not highly restricted. See ROBERT K. CARR, THE HOUSE COMMITTEE ON UN-AMERICAN ACTIVITIES, 1945-1950, at 253-61 (1952); AMERICAN CIVIL LIBERTIES UNION, THE CASE AGAINST THE HOUSE UN-AMERICAN ACTIVITIES COMMITTEE 17-23 (1964).

[106] The Committee described its post-war program as one to "expose and ferret out" and to "spotlight" communist activities, along with its "continued accumulation of files and records to be placed at the disposal of the investigative units of the Government and armed services." The language comes from a 1948 report by the Committee to the House, quoted by Mr. Justice Harlan in Barenblatt v. United States, 360 U.S. 109, 119 n.11 (1959).

[107] The dissenting opinion of Mr. Justice Clark helped to reinforce this mistaken impression, arguing that "Unless the Congress changes the rule announced by the Court today, those intelligence agencies of our Government engaged in law enforcement may as well close up shop, for the Court has opened their files to the criminal and thus afforded him a Roman holiday for rummaging through confidential information as well as vital national secrets." Jencks v. United States, 353 U.S. 657, 681-82 (1957) (dissenting opinion).

ate to discuss both public and private repositories of personal data. The suggestions below are designed in part to provoke responses from those whose concerns and responsibilities are more immediate.

A. Criminal Records and Law Enforcement Agency Files

Three roughly-defined classes of records may be identified in the area of law enforcement: First, there are the "raw" investigative files of police agencies; such a file

> may contain information that is false, trivial, or perhaps malicious. It also includes reports on administrative details in the investigation, the investigative techniques used, and the identity of informants.[108]

When a criminal proceeding is begun, much of the material in a file of this kind becomes part of the prosecuting attorney's case file. Present administrative policy universally aims at tight security, limiting access to investigative files to the police personnel who make the investigations and to the attorneys who prosecute each case. Even within a given law enforcement agency, the official policy is to deny access to members of the agency who are not part of its investigative branch, absent special high-level permission. A few detectives from other police agencies may be authorized such access, but their numbers are limited. Nonetheless, it is probably true that some private investigators with the proper contacts can obtain information from these investigative files.[109]

Next, there are the routine records that are the daily grist for the paper mill that characterizes big-city law enforcement agencies: fingerprints,[110] photos, arrest and conviction records. These are not public records. But any private investigator worthy of the name can get access to the information on anyone's "make sheet": arrests, detentions which are "not deemed" arrests, convictions. Finally, there are the court records in criminal cases. These are public records, with occasional exceptions in cases dealing with some sex offenses.[111]

---

[108] DON WHITEHEAD, THE FBI STORY 289 (1956).

[109] One important exception to this rule appears to be the investigative information compiled in special police intelligence units that keep track of persons thought to be involved in organized crime. Another seems to be the files of the FBI, at least with respect to private investigators. See PACKARD, *op. cit. supra* note 91, at 161, quoting a famous private investigator; see also WHITEHEAD, *op. cit. supra* note 108, at 84. Congressional committee investigators may find the FBI more cooperative. "The closest relationship exists between this committee [the House Committee on Un-American Activities] and the FBI . . . . It is something, however, that we cannot talk too much about." Chairman J. Parnell Thomas, quoted in COOK, *op. cit. supra* note 83, at 289.

[110] On June 30, 1965, the FBI had more than 175 million fingerprints on file, covering over 78 million persons, nearly 16 million of whose prints are in the "criminal files." The civil files are not searched except in special cases, such as identification of dead bodies. FBI ANN. REP., FISCAL YEAR 1965, at 36. COOK, *op. cit. supra* note 83, at 215-16, is critical of the FBI's failure to weed out its fingerprint files, citing a Scotland Yard authority for the proposition that "Weeding is essential" to save search time. The advent of the computer invalidates that criticism. For full description of the FBI's fingerprint activities, see Hoover, *The Work of the Fingerprint Division of the Federal Bureau of Investigation*, The Student Lawyer Journal, Oct. 1961, p. 13; WHITEHEAD, *supra* note 108, ch. 15.

[111] The Los Angeles County municipal courts make use of a new central traffic index, for the purpose

What is suggested here is essentially a codification of existing practice (as distinguished from stated policy), with an effort to trim some ragged edges. Court files should remain public records; California's recent record-sealing legislation, discussed below, goes to—perhaps beyond—the limit of justifiable protections of reputations by suppressing the truth, and should not be extended. The raw investigative files, and prosecutors' case files, should be strictly confidential—subject, of course, to the normal rules of criminal discovery.[112] Access should be granted to other law enforcement agencies only upon approval at a high administrative level within the agency that holds the investigative file.[113] I do not mean simply that the officially stated policy of the various law enforcement agencies should be that such files are confidential; I mean that a range of disciplinary sanctions should be established and enforced within each agency, so that persons in a position to divulge information improperly will know that they run a serious risk in doing so. The objective here is a credible deterrent, a substantial increase in the cost of access. The maximum administrative penalty for wrongful disclosure should therefore be dismissal. Furthermore, the victim of such a disclosure should be permitted to sue for a statutory penalty—say, $1,000—in addition to compensatory damages for any actual harm he can demonstrate.[114]

The foregoing suggestions require no change in present stated policy and only a minor change in enforcement practice. The suggestion that follows, on the other hand, calls for a modification of stated policy to bring it in line with current practice. It is that access to such routine information as that contained on "make sheets" be

of exchanging information concerning traffic offenses and their dispositions by the various courts. CAL. GOV'T CODE § 72623.

[112] See Louisell, *Criminal Discovery: Dilemma Real or Apparent?*, 49 CALIF. L. REV. 56 (1961).

[113] Even this suggestion has its difficulties. We can hardly expect the various police departments around the country to refuse to share investigative leads among themselves. Yet there are serious possibilities of abuse. One recent example was the rather interesting use made of an old criminal file of Mrs. Viola Liuzzo, the victim of a murder charged to certain members of the Ku Klux Klan (one of whom was acquitted by a Lowndes County, Alabama, jury). Mrs. Liuzzo's record (her "make sheet," *not* an investigative file) somehow passed from the Detroit police to the Warren, Michigan, police, to Sheriff Clark of Dallas County, Alabama, and even on to Imperial Wizard Shelton of the KKK. See N.Y. Times, May 16, 1965, p. 51, col. 1.

The point is that some policemen, like others in all occupations, can be expected to make improper use of information in police files. There are organizations of policemen which are highly politically oriented. One example in my area is the Fire and Police Research Association of Los Angeles, Inc. (FI-PO), which engages in right-wing political activity, including the publication of *The FI-PO News*, a newsletter which consists in substantial part of lists of names of persons who have been identified by someone as communists or communist sympathizers, often coupled indiscriminately with the names of persons who support the establishment of civilian police review boards, and so on. The leaders of FI-PO are men in responsible positions in the police and fire departments of Los Angeles. I am morally certain that FI-PO has access to any police file in the city. The Liuzzo incident suggests that such organizations may have ready access to some police records all over the country. But any system that required proof of legitimate need before investigative information could be exchanged with other departments would be costly in both money and investigative efficiency; it is doubtful that our various city councils would (or should) be willing to pay the price.

[114] Some decisions imposing tort liability for violation by public officials of nondisclosure statutes are collected in Annot., *Constitutionality, construction, and effect of statute or regulation relating specifically to divulgence of information acquired by public officers or employees*, 165 A.L.R. 1302, 1304-05 (1946).

allowed freely to outside investigators, public and private alike. Probably access should be restricted to licensed private investigators to keep idle snooping at a minimum.[115] But credit and business investigators, private investigators in domestic relations cases, and the like should be allowed in law what they now have in fact. The corroding, demoralizing occupation of information-peddling within police departments would thus be struck a near-mortal blow.

This proposal is seriously made in awareness of the terrible consequences of the publication of arrest records to prospective employers and others who deal with the subjects of such files. Thousands upon thousands of injustices are surely done each year because isolated instances of youthful misconduct permanently brand otherwise useful and honorable citizens and because "police records" are hung about the necks of innocent victims of mistaken identity and other inevitable errors in so human an institution as police work. A concern for those victims naturally produces calls for corrective legislation.[116] But the predictive assumption that legislation forbidding disclosure of arrest records would achieve its goal is an optimistic one and one that I do not share. Access to "make sheets" within the agencies has not been severely limited, and the offense of disclosure is so widely practiced now that it must seem to many policemen to be a pure case of *malum prohibitum*. The same cannot be said of investigative files; access practices and attitudes are different, and a firmly enforced limitation on access would be both practical and acceptable. In fact, the principal advantage of formally recognizing a right of access by outside investigators to routine information, such as arrest records, would be that a clear separation might be made in the minds of agency personnel between the information in such records and that in investigative files. At present, both kinds of information are theoretically confidential; one disclosure is theoretically as improper as another. Ironically, the most likely result of the proposed change would be a net increase in the protection of the confidentiality of personal data in the hands of law enforcement agencies.

The same separation of the two kinds of personal information in police files will materially aid in improving the files' accuracy. The subject of the file should have access to his own "make sheet"—at intervals of six months or a year, in order to avoid the cost involved in frequent requests. The "make sheets" are already transmitted as a matter of course to other agencies; they are duplicated for that purpose, and it will not cost much to make the subject a copy and to give him a copy on request. The principal cost will be that of interrogating the file; soon, however, that task can be assigned to automated means. In fact, "make sheets" and similar routine information will be the first criminal data to be stored on computer tapes.[117] The

[115] Such a limitation would roughly parallel the various interests protected by the qualified privileges in the law of defamation.

[116] *E.g.*, Comment, *Guilt by Record*, 1 CALIF. WESTERN L. REV. 126 (1965).

[117] See HEARLE & MASON, *op. cit. supra* note 5, at 120-22. It was the storage of this kind of routine information in a computer that led to the recent nationally-publicized arrest of a New York City lady

subject himself is the best assistant the police agency can have in clearing up cases of mistaken identity or other omissions such as acquittals or other dispositions favorable to him.[118]

It is not suggested that the subject should have access to his investigative file beyond that permitted by the ordinary rules of criminal discovery, which apply only when the subject is a defendant in a criminal proceeding. It is true that some inaccuracies will be cleared up by the subject, but the risk of compromising investigative leads and the identity of useful informers outweighs the subject's interest in statements in the file made by witnesses who testify against him, as the *Jencks* decision held[119] and as Congress soon thereafter provided in the Jencks Act.[120] Conversely, when the government seeks to use a statement in the file against the subject in an administrative proceeding, without permitting him to know the contents of the statement or the identity of its author, the subject should have access to the full statement and an opportunity to cross-examine the witness. In *Greene v. McElroy*,[121] the Supreme Court rested such a right of confrontation on nonconstitutional grounds, interpreting the existing federal loyalty program legislation and regulations. The principles of the *Jencks* and *Greene* cases are worthy of general application, but they do not support a rule of a general right of access by the subject to law enforcement investigative files. Of course, access by the subject to his own "make sheet" does not involve the same risks of compromise to the agency's investigative functions.

In *The Naked Society*, the most recent entry in Vance Packard's series of glossy exposés, we are told that it is important to protect privacy in order to protect "the right to hope for tolerant forgiveness or overlooking of past foolishnesses, errors, humiliations, or minor sins—in short, the Christian notion of the possibility of redemption"

---

after sixteen months of neglect of a traffic summons. She had been identified by her license number, called out by a policeman over the radio to a computer center which processed the number in seconds. See *The Computer & Mrs. Placente*, Time Magazine, Sept. 3, 1965, p. 72, col. 1. During the same month, IBM advertised the use of its computers to "help keep track of pawnshop records, gun licenses, stolen property reports, violations and arrests," as well as "to find *at once* a set of matching fingerprints from files of tens of thousands." The Atlantic, Sept. 1965, p. 61.

[118] In California, where all arrests are reported to the state's Bureau of Criminal Identification and Investigation, the law also requires a follow-up report of each release without charge, and each disposition by a criminal court. CAL. PEN. CODE §§ 11000-15.

[119] Jencks v. United States, 353 U.S. 657 (1957).

[120] 18 U.S.C. § 3500 (1958). It is mystifying that Fred J. Cook should describe this legislation as a "defense-crippling law," secured by Director Hoover to "nullify the Court's Jencks decision." COOK, *op. cit. supra* note 83, at 385, 389 (1965). Mr. Cook's concern is that the FBI agent may not have the informer sign or "adopt" his statement when it is reduced to writing, so that the act will not require its production. But such an unsigned statement might still be ordered to be produced by the trial judge, and indeed such an order may be compelled by the Constitution. See the concurring opinion of Mr. Justice Brennan, joined by the Chief Justice and Justices Black and Douglas, in Palermo v. United States, 360 U.S. 343, 361-62 (1959). This decision, upholding the constitutionality of the Jencks Act, is described by Mr. Cook as one in which "the Court, in effect, reversed itself . . . ." Perhaps Mr. Cook, like those he criticizes, has taken Director Hoover's reaction to the *Jencks* decision too seriously. Mr. Justice Brennan's concurring opinion in *Palermo* seems certain to prevail in the future.

[121] 360 U.S. 474 (1959), decided on the same day as the *Palermo* case.

and "the right to make a fresh start."[122] Substantial agreement with this point of view has produced legislation in California which, without authorizing destruction of records, approaches the ultimate in legislative restrictions on access to personal data. Since 1909, the state has adopted an official posture of forgiveness for defendants who have been convicted of crime but who have been placed on probation and have successfully completed the period thereof. Such a person may apply to the court that convicted him for relief, which the court "shall" grant: he may withdraw his plea of guilty, or the court will set aside a verdict of guilty; in either case, the court will dismiss the criminal charge. The defendant "shall thereafter be released from all penalties and disabilities resulting from the offense or crime of which he has been convicted."[123] That statute, considered alone, forgives without forgetting. The defendant's fresh start is significant but hardly complete. His forgiven conviction may be pleaded and proved as a prior conviction;[124] it may be made the basis for deportation,[125] or the suspension or revocation of a driver's license, or a professional disciplinary proceeding.[126] Furthermore, the record of conviction is a public record, open to inspection along with other court records and thus available to any investigator on behalf of a prospective employer, or lender, or participant in a business transaction. In short, the earlier legislation did not "expunge" the conviction.[127]

To make the forgiveness more effective in some cases, the California legislature has recently enacted a new remedy, applicable only to misdemeanors or juvenile offenses committed by minors but extending to arrest and custody records as well as records of conviction or commitment to the Youth Authority. If the offense is the minor's only one,[128] he may, in the case of a criminal proceeding,[129]

> petition the court for an order sealing the record of conviction and other official records in the case, including records of arrests resulting in the criminal proceeding, and including records relating to other offenses charged in the accusatory pleading, whether defendant was acquitted or charges were dismissed.[130]

---

[122] PACKARD, *op. cit. supra* note 91, at 12. Connoisseurs of the law reviews are directed to Professor Joseph Bishop's delightful review of this book in 74 YALE L.J. 193 (1964).

[123] CAL. PEN. CODE § 1203.4.

[124] *Ibid.*

[125] Garcia-Gonzales v. Immigration & Nat. Serv., 344 F.2d 804 (9th Cir.), *cert. denied*, 382 U.S. 840 (1965); Kelly v. Immigration & Nat. Serv., 349 F.2d 473 (9th Cir.), *cert. denied*, 382 U.S. 932 (1965). Both decisions are reluctantly supported in Comment, *The Futile Forgiveness: Basing Deportation on an Expunged Narcotics Conviction*, 114 U. PA. L. REV. 372 (1966), with a call for congressional revision of the governing law.

[126] Meyer v. Medical Bd., 34 Cal. 2d 62, 206 P.2d 1085 (1949).

[127] See Baum, *Wiping Out a Criminal or Juvenile Record*, 40 CALIF. S.B.J. 816, 819 (1965); Booth, *The Expungement Myth*, 38 L.A.B. BULL. 161 (1963).

[128] The statute denies the record-sealing relief to "a person convicted of more than one offense." Baum, *supra* note 127, at 823, persuasively argues that it is logical to interpret the language to refer not only to other convictions in the same proceeding but also to previous convictions.

[129] The parallel provision relating to juvenile records, enacted before the quoted provision concerning criminal convictions, is CAL. WELFARE & INSTITUTIONS CODE § 781.

[130] CAL. PEN. CODE § 1203.45.

The court "may" grant the relief sought. If it does,

> Thereafter such conviction, arrest, or other proceeding shall be deemed not to have occurred, and the petitioner may answer accordingly any question relating to their occurrence.[131]

Thus is the slate wiped nearly clean—nearly but not entirely. It is true that notices of the sealing of records are sent to the agencies that have previously received notice of the arrest, conviction, or juvenile proceeding.[132] It is true also that the custodians of such derivative records should answer to inquiry, "We have no record on the named individual."[133] But the California legislature cannot authoritatively tell the FBI or the Nevada police to seal their records. And between the time when an arrest or conviction takes place and the time when the records are sealed, many a private investigator will have had the chance to make his own notations, which can then be passed on and on. Indeed, the very existence of this new remedy will create pressure on private investigative agencies to make records immediately after a minor's conviction, taking advantage of the services of court reporting firms. In the words of Mr. Terry L. Baum, Deputy Legislative Counsel of California, "It seems that when the Moving Finger writes these days, a dozen Xerox copies likely are made."[134] In a completely automated world, in which all personal data files were unified in one electronic data bank, an erasure might be made effective. Until that unhappy day arrives, the erasure attempted by California is most unlikely to work.

Suppose, however, that it were effective. Has the California legislature chosen the right remedy to protect the youthful offender? The new legislation is no doubt constitutional, by analogy to a great many decisions upholding the validity of restrictions on disclosure of information in the hands of public officials.[135] So long as suppression is not made of information closely related to public affairs, no constitutional challenge to this record-sealing legislation is likely to succeed. But much is constitutional that is not wise. Even a benevolent falsification of history should be undertaken only for the most compelling reasons. Perhaps no amount of explaining will convince a prospective employer that a young man has been rehabilitated. Still it is highly questionable whether the state should deny the employer the information upon which to make his own decision.

If there were no alternative means for avoiding the undesirable result of a permanent disqualification for certain kinds of employment, or other harm to the youthful offender, the solution chosen by the California legislature would be more acceptable. There are, however, such alternatives. A refusal to employ that is based on a conviction for a misdemeanor committed before the applicant reached twenty-

[131] *Ibid.*

[132] CAL. PEN. CODE §§ 11105.5, 11116. The court records themselves are to be "sealed"—closed to inspection—but are not to be destroyed. 41 OPS. ATT'Y GEN. CAL. 102 (1963).

[133] 40 OPS. ATT'Y GEN. CAL. 50 (1962); 41 *id.* 102 (1963).

[134] Baum, *supra* note 127, at 824.

[135] See Annot., *supra* note 114. *But see* text accompanying note 28 *supra*; Franklin, *supra* note 34.

one might be made an unfair employment practice. If the concern is that enforcement of such a rule would be difficult, employers might even be forbidden to ask whether applicants were so convicted. The latter alternative also involves some impairment of the constitutional interests in a free flow of information, but it has two important advantages over the California statute: First, it is less of a limitation on access to information, because it is limited to employers' inquiries. Second, even if the legislature were to make a list of several situations in which such an inquiry would be forbidden, the making of that list would require the legislature to give specific consideration to each claimed need for restricting the flow of information. The California law is not so limited, nor has it been drafted with specific evils in mind. The effect of the law is to put the information in a box, where no one can reach it—unless, of course, a credit investigator has picked up the news of the conviction before the record was sealed, in which case anyone who makes a serious inquiry will know about it. The statute is at once too broad a restriction on the exchange of information and too narrow in scope to be effective.

B. Consumer Credit Investigation Files

The credit manager who approves an application for retail credit is gambling on the future; in betting the amount of the loan against the possibility of repayment with interest, he necessarily makes a complex prediction about the prospective purchaser. He wants the prediction to be an informed one—informed, that is, by experience, both of the lender and of the borrower. The relevant information about the borrower has been reduced, in the jargon of credit men, to the "Three C's": Capital (the borrower's net worth), Capacity (his ability to earn in the future), and Character (principally his past debt-paying record, but the use of such a morally evocative term implies that other considerations are also thought relevant).[136]

Some retailers run their own credit investigations; most, however, make use of the services of the more than 2,000 independent credit bureaus which are members of a trade association called the Associated Credit Bureaus of America, Inc. (ACBA).[137] In 1961, Hillel Black wrote of the ACBA that its

> credit bureaus alone employ an army of seventeen thousand who furnish nearly sixty-seven million oral and written credit reports a year . . . . [T]he credit records of the Association's members number seventy million. Since many records contain the personal and financial background of both husband and wife, the number of histories in the credit bureau's [*sic*] files of the United States total one hundred and ten million . . . . If your name is not in the records of at least one credit bureau, it doesn't mean that you don't rate. What it does mean is that you are either under twenty-one or dead.[138]

[136] See HILLEL BLACK, BUY NOW, PAY LATER 46 (1961).

[137] There are, in addition, other bureaus which are not members of the association.

[138] BLACK, *op. cit. supra* note 136, at 36-37.

The number of files and reports increases with the population, for almost everyone buys something on credit.[139] The typical file contains the basic information that a credit manager wants: "name, age, residence, marriage, divorce, inheritance, earnings, criminal record, bank account, date debts assumed and paid, slow pay, fast pay, no pay."[140] The information in the file is routinely available to bureau subscribers, and to law enforcement officers, including revenue investigators. It is also available, not routinely but just as certainly, to anyone else who can pay the modest going rate.[141] Thus credit bureau files are the basis for many another investigative file, or, in Myron Brenton's phrase, "credit builds the goldfish bowl."[142]

The fact that access to credit reports is virtually unlimited makes the accuracy of the reporting particularly important. Practices vary from one bureau to another, but generally the investigator enters his own evaluations, along with those of the references supplied by the subject, and not simply a narrowly factual account of his payment history. I have a copy of a 1962 credit report (with the name obliterated, speaking of privacy invasions) from Columbus, Ohio. It is a standard form which purports to be supplied by the ACBA. Under the heading "Character," these questions appear:

7. Is applicant well regarded as to character, habits and morals?
8. Did you learn of any domestic difficulties?
9. Does he have a reputation of living within his income?

The reports from previous credit sellers are entered in terms such as these: "satisfactory," "a little slow," "paid slow." Practices are not uniform among sellers, and "slow" does not have a universally accepted meaning.

Old derogatory entries may remain in the subject's file long after their causes are thought to have been "cleared up," for example, by payment or by successful termination of a lawsuit over a disputed claim. But the practice of the largest credit bureau (that of New York) is to eliminate old reports on a regular basis after five or ten years.[143] Once a clear inaccuracy is called to the attention of a bureau, it is corrected; the bureaus earn their living by their reputation for accurate reporting.[144] If there is a disputed claim, however, the credit bureau is not likely to remove the retailer's "no pay" evaluation even though the subject of the file has returned the merchandise on the ground that it was defective. The bureau does not want to put

[139] Even teenagers. See BLACK, *op. cit. supra* note 136, ch. 7, for a depressing explanation of current techniques for introducing children to consumer credit as "a way of life."

[140] *Id.* at 40-41.

[141] "I tried to purchase [credit] reports from five suburban credit bureaus east of the Rocky Mountains, in each case explaining that I contemplated going into partnership with someone but wanted to check up on him beforehand. Only two bureaus refused to sell me a report." BRENTON, *op. cit. supra* note 91, at 36.

[142] *Id.* at 25-43.

[143] BLACK, *op. cit. supra* note 136, at 41.

[144] While it is true that credit bureaus' form contracts include disclaimers of liability to their customers for inaccurate reporting (see PACKARD, *op. cit. supra* note 91, at 172; AM. JUR. LEGAL FORMS, Mercantile Agencies 9:41), most bureaus are zealous to avoid errors. *Cf.* Green, *The Duty to Give Accurate Information*, 12 U.C.L.A.L. REV. 464 (1965).

itself in the position of a tribunal which litigates such questions; if it were to do so, the cost of credit reporting—and thus the cost of merchandise to the consumer[145]—would be somewhat increased.

The applicant for credit knows that the credit seller will make some inquiry of the references he has supplied; typically, those references are the applicant's bank, his employer, and firms that have granted him credit in the past. The applicant may not know that the bank will go beyond verifying that he has an account, giving the inquiring retailer or credit bureau a rough estimate of the average balance.[146] The consent that the applicant gives for access to the information is thus imperfect, and that imperfection is compounded by his lack of awareness of the ease with which others wholly unrelated to the credit transaction may have access to information in the hands of the credit bureau.[147]

The foregoing description of current practice relating to credit information, like those of recent viewers-with-alarm, may seem to be an introduction to a call for legislative action of a fundamental kind. It is not. The information in standard credit bureau files (as distinguished from those resulting from "special" investigations[148]) is not overly sensitive. Only in relatively few cases are requests for credit reports made by persons other than those who have been asked to give the subjects credit, others similarly situated (such as insurers), or law enforcement officials. A law that required proof of need to know or required permission from the subject for each credit report would be expensive. Credit bureaus provide much of their information to subscribers over the telephone. Even if the crudest sort of control were provided—a call-back system to identify the caller, for example—the number of phone calls would be doubled. Even that control would not prevent a subscriber from passing on the information to someone else. A control system based on "instant consent" of the credit applicant would require elaborate schemes to identify the person who claims to be the subject of the file, such as a card that could be inserted in a telephone, or perhaps a voice-identification system, with corresponding losses of privacy for the purposes of identification. Finally, special protections would have to be devised for the interstate information request. At present, inter-bureau exchanges

[145] Not just the credit consumer but all consumers. In most retailing operations, cash customers pay a substantial part of the cost of credit selling.

[146] Perhaps in Idaho this practice has been curtailed by the remarkable decision in Peterson v. Idaho First Nat'l Bank, 83 Idaho 578, 582, 367 P.2d 284, 286 (1961), annotated in 92 A.L.R.2d 891 (1963). The Idaho court held that the plaintiff had stated a cause of action by alleging that the bank had disclosed ("with malice and without authorization of the plaintiff") to the plaintiff-depositor's employer, the fact that the plaintiff had written "a large number" of insufficient-funds checks. The employer had a few months previously, asked the bank to report whenever an employee "might be doing anything that might bring discredit to the company." The cause of action was rested on a theory of breach of an implied contract to keep the depositor's bank-transaction information confidential; the court rejected an invasion of privacy theory because the information had not been made "public." *Id.* at 582, 367 P.2d at 386.

[147] Including "slow pay" reports from previous creditors whose names he did not give as references.

[148] See PACKARD, *op. cit. supra* note 91, ch. 10, for a description of special investigations of an elaborate character by insurance investigators. Credit "specials" are less detailed.

of credit data are routinely given.[149] A national enforcement system to give teeth to access controls is most unlikely. Does that imply that there will be a Reno for credit data? One local control over the export of credit data might take the form of an insistence that an out-of-state request for the data be accompanied by written permission of the subject of the file or an identification of the requesting bureau's customer and a demonstration of the customer's need to know. But at what cost are we willing to impose controls of that kind?

Beyond the very considerable money costs imposing effective limits on access to credit information, there are hidden costs of another type, which are hard to estimate. To the extent that Adam Smith's "invisible hand" continues to guide the economy, there is a vital interest in a friction-free flow of information that is relevant to individual economic decision-making. The data in credit bureau files should be readily available to those who find it useful in making such decisions. A poor credit risk who fails to repay his loan burdens the whole economy; if subsidies of that type are to be paid, they should be identified and evaluated as such and not hidden in the price of all consumers' purchases.

It is not argued that the idly curious should be encouraged to snoop. One institutional protection that deserves consideration is a requirement of notice to the subject of the file that a credit report has been made—arguably excluding reports to the police.[150] That, too, involves additional expense to the consumer however the cost of the notice is initially absorbed. The notice might be given in the form of a quarterly list of all those who have requested and received reports. In whatever form it is given, a notice of this kind would certainly discourage inquiries for essentially social reasons, as where the parents of the girl check on the credit rating of the parents of the boy.[151]

The credit bureaus do not, as a matter of course, send each subject a copy of his own credit report. Access is so easy, however, that anyone who wants to see his own file can do so at low cost. Perhaps that cost to the subject should be eliminated, so that he might be entitled to a copy of his file once in a specified period, such as a year. Perhaps also this free access to the subject should be limited to certain critical occasions, such as the denial of credit. However the subject gains access to his own

[149] BRENTON, *op. cit. supra* note 91, at 28, says that the ACBA bureaus "provide approximately 7,500,000 interbureau reports annually."

[150] In Wisconsin, state income tax and gift tax returns were at one time open to public inspection. Anyone could inspect anyone else's return, but immediate notice was sent to the taxpayer of the name of each person who inspected his return and the reason for the inspection. Wis. Laws 1951, ch. 714. In 1953, the law was amended to permit access only to the amount of income tax or gift tax paid, with the same provision for disclosure of the identity of the person to whom the information is given and his stated reason for inquiring. Nonresidents are not allowed to receive this information unless their states make similar information available to Wisconsin residents or corporations. Wis. Laws 1953, ch. 303, now in WIS. STAT. § 71.11(44)(b), (bm) (1963).

[151] Such instances are related by BRENTON, *op. cit. supra* note 91, at 36-37. The problem of interstate exchanges of credit information would still remain, and may be insoluble. One who wishes to know of another's credit standing without disclosing his inquiry can employ enough intermediaries to insulate him from that disclosure.

file, he should have the right to add a statement of moderate length about any derogatory entry that he thinks creates an inaccurate impression if left unexplained. The removal of claimed inaccuracies should not be required; however, once the subject has notified the credit bureau that he considers a derogatory entry to be false, the bureau may have difficulty in establishing its qualified privilege in a later defamation action based on the publication of the disputed entry.[152] There are a great many cases which hold that "malice" which overcomes the asserted privilege may be established by proof of a reckless disregard of the likelihood that the derogatory information is false.[153] The award of damages in cases of that kind may be a risk that credit bureaus are willing to run in order to serve their customers. Such damages, like other costs of doing business, will surely be paid by consumers in the end, but that is a more attractive result than leaving the loss where it has fallen, on the victim of the defamatory report.

Any institutional suggestions in the area of credit reporting are short-term proposals. Here, as much as anywhere, "the rate of change of technology and society threatens to make footless fantasying of any speculations about the impact of selected factors."[154] For a radical restructuring of the whole consumer credit system seems to have begun. Retailers as a class have already begun to withdraw from the credit business in favor of financial institutions. The credit card is gradually replacing the charge-a-plate and bids fair to replace the personal check.[155] Tomorrow's consumer will have one cash-credit account with one financial institution. When he buys a suit, the salesman will insert the customer's cash-credit card in a slot in a telephone, dial the appropriate numbers to represent the amount of the sale, and wait for an approving signal from the bank's computer. The customer's bank account will be reduced—or his loan account charged. The retailer will have loaned no money; for him, every sale will be a cash sale. Thus he need not make a credit investigation.

In fact, no one need make a credit investigation relating to the granting of consumer credit, except for the bank. What kind of investigation will the bank make? When it accepts a customer for an account which authorizes loan-overdrafts ("In-

[152] In 1965, a bill was introduced in the California legislature to "require" credit bureaus to correct any false report. The sanction for failing, after notice, to disseminate the corrected report to recipients of the false one was to be loss of the qualified privilege (the common law privilege written into statute by CAL. CIV. CODE § 47(3), A.B. 920, 1965 Regular (General) Sess.). The bill was not enacted into law, but much of its substance could be achieved by judicial decision within the existing law of defamation. *Cf.* Stationers Corp. v. Dun & Bradstreet, Inc., 62 Cal. 2d 412, 42 Cal. Rptr. 449, 398 P.2d 785 (1965) (using the expression "probable cause" to describe the non-"malicious" state of mind). See also Annot., *Libel and slander: report of mercantile agency as privileged*, 30 A.L.R.2d 776 (1953).

[153] Even negligence is enough to overcome the privilege in some jurisdictions. See Hallen, *Character of Belief Necessary for the Conditional Privilege in Defamation*, 25 ILL. L. REV. 865 (1931). It should be added that there are some decisions to the effect that it is not libelous to impute a low credit standing to one who is not a merchant. See Annot., *Imputing credit unworthiness to nontrader*, 99 A.L.R.2d 700 (1965).

[154] Michael, *supra* note 84, at 270.

[155] See *Check Writing Seen Being Reduced Sharply "In Foreseeable Future,"* Wall St. Journal, Feb. 10, 1966, p. 4, col. 3.

stant Money," in the promotional material of at least one bank[156]), it will be entering into a relationship which may be a lifelong one. The initial investigation will probably be more thorough than the investigation now made of a typical credit buyer. But soon the bank will have built up its own body of experience with the customer. Its own records will provide his complete financial history, superior to what a credit bureau can now produce at comparable cost. When the customer begins to look like a "no-pay," the bank can tug at the string. If he goes elsewhere in search of credit, the new bank will ask the old one for his record. If the customer moves to another city, his bank-credit record will tag along. It may become necessary to police concerted denials of credit as other concerted refusals to deal are now policed.[157] But access to the information will otherwise be more easily controlled. Without question, it will cost more than ten dollars to get a bank-credit file in that era of centralized credit and centralized data processing. At the same time, inaccuracies in the files will almost certainly be reduced. It will be to the bank's advantage to provide its customers with cash-credit statements, to assist in keeping him within his means. There will be little need for evaluative reporting; disputes over the quality of merchandise bought with borrowed money will be none of the bank's concern, and a credit buyer will not be called a "slow pay" because he tried to get his money back from the retailer.

CONCLUSION

One need not believe, as I do on my gloomier days, that we are marching steadily to the Anthill in order to share the view that our main concern about "the files" should be directed to their accuracy, not to their accessibility. Any society, whatever its degree of freedom, has a great deal to gain from unimpeded access to information. Any society risks serious losses in the quality of low-level decision-making if its leaders decide before the event that certain classes of information must be kept secret because they will not be relevant to future decisions. In the society of the near future, much more personal information will be relevant to predicting individual performance. Concurrently, much more will be thought to rest on predicting accurately. Whatever we do today to restrict access to personal data, our successors will probably discard. The same cannot be said of efforts to make the files accurate. If there is one sure, positive contribution we can make to those who follow us, whatever social forms they choose, it is to make all our reservoirs of information into truer reflections of the world we see.

[156] See BLACK, *op. cit. supra* note 136, at 118-22.

[157] *E.g.*, Ruddy Brook Clothes, Inc. v. British & Foreign Marine Ins. Co., 195 F.2d 86 (7th Cir. 1952) (injunction under Clayton Act against blacklisting by fire insurance companies).