AUTOMATED DATA PROCESSING AND THE ISSUE OF PRIVACY

*Arthur J. Sills**

From a strictly scientific and technical vantage point, it appears at this moment in history there are no limits to the precision and extent to which information may be gathered, stored, collated, and disseminated by mass data processing systems. Perhaps the most current and extensive manifestation of this potential is evidenced by the proposed National Data Bank which would pool and standardize statistics from twenty federal agencies.[1] These would include, among others, the Census Bureau, the Internal Revenue Service, the Bureau of Labor Statistics, the Office of Business Economics, the Federal Reserve Board and the Bureau of Old Age and Survivors Insurance. These government agencies now have 100 million punch cards and 30,000 computer tapes containing information about people and companies.

Furthermore, a system of this sort could readily be adapted to include other federal agencies, and could be tied into a massive network of federal, state, and local data systems. The mere participation of the Department of Defense would add 14 million life histories to the pool. Civil Service would add 8 million more. No one is sure how many personal files the F.B.I. has, but this agency will admit to information on 100,000 "Communist sympathizers." If we proceed further to include the likes of Social Security records, police records, medical and others, including personnel and job files, there would be an estimated 2.8 billion listings available through a centralized data bank.[2]

Heretofore, persons concerned with the use and preparation of automated data processing systems have concentrated primarily on a wide span of technical and scientific considerations. State legislators and State administrators, alike, have focused on ADP equipment, on standardization and coding of information, and on intergovernmental cooperation in the field. Training and education of ADP operators and programmers and retraining of personnel displaced by ADP have been additional subjects of concern. It can fairly be said, however, that the primary emphasis has been on what we could call the nonhumanistic

---

* Former New Jersey Attorney General, Mr. Sills was the recipient of the Brown Memorial Award for his literary accomplishments in this field.

1 N.Y. Times, Jan. 7, 1968, at 1, col. 6.

2 *Id.*

aspects of data processing. The situation is very much analogous to the scientific and technical effort made decades ago to harness nuclear energy with human considerations at that time being but a mere afterthought.

With respect to mass data gathering, we have also known that very important human concerns are involved—especially for invasion of privacy that has been occasioned by the data processing revolution. This potential now requires increased attention. It will necessitate suitable responses if we are to cope with a challenge to the foundations of our democratic institutions themselves.

Advances obtainable from ADP can be desirable. They can serve to further the progress of our communities. Better information no doubt will provide better understanding of the interdependencies within our pluralistic society, leading to better informed choices.[3] Increased accessibility of data, coupled with budgetary and spatial savings, will enable government to remain abreast of the future demands of its citizens and improve existing services. Extensive utilization of raw data in the virtually untapped field of behavioral research should provide more accurate forecasting potential in such areas as manpower skills and their availability, population concentration and dispersements, transportation patterns, health services, law enforcement and control of criminal activity—to cite a few examples in a practically limitless field.

This technological revolution cannot be ignored. But has it any limits? If it does, or if it should, then we must commit ourselves to begin to define the nature of these limits, and to inquire to what extent the limits can be accommodated or harmonized with the expanding technology.

In analyzing privacy, it is most meaningful to see it in its broadest aspect: namely, to determine what role it plays in the society. In order to see that role, in our democratic society, it may be helpful by way of contrast to describe the antithetical posture it maintains in a totalitarian regime.

The modern totalitarian state relies, in varying degrees, on secrecy for the regime and full surveillance for all other groups. Both Fascist and Communist literature are replete with attacks on the idea of privacy as "immoral," "antisocial," and part of "the cult of individualism." In the consolidation phase, totalitarianism commands that traditional confidential relationships be destroyed, surveillance systems and

---

3 *The Design of a Federal Statistical Data Center*, National Bureau of Standards as reported in the *Hearings of Subcommittee of the Committee on Government Operations, House of Representatives*, 89th Cong., 2nd Sess. at 294 (1969).

informers installed, thorough dossiers compiled on its citizens, and privacy denied. Affirmative and unwavering loyalty is exacted, which tends to isolate the citizen; he, in turn, seeks refuge in the state and identifies with its programs. Although a certain degree of privacy is permitted following consolidation of power, the primary surveillance systems of paid and voluntary spies, eavesdropping and watching devices, and strict records control, are retained to keep the regime on its guard.[4]

Professor Westin has said: "Just as a social balance favoring disclosure-surveillance to the exclusion of privacy considerations is a functional necessity for totalitarian systems, so a balance that insures strong citadels of individual and group privacy and limits both disclosure and surveillance is a prerequisite for liberal democratic societies. The democratic society relies on publicity as a control of government and privacy as a shield for group and individual life."

A democratic system encourages personal retreat for the individual, to secure perspective and critical judgment. A strong commitment to the family as a basic, autonomous unit responsible for important educational, religious and moral roles is recognized. Consequently, claims to physical and legal privacy against society and the state help to preserve the family relationship intact. Religious diversity and ideas of toleration guarantee that religious choice is a matter of private concern. The citizenry is afforded a wide freedom to join associations and participate in group affairs; to this end, privacy of membership and intra-group action is protected. Maximum freedom for political choice is assured by providing a secret ballot and by forbidding governmental inquiries into a citizen's past voting record. Through a constellation of political, legal and constitutional restraints, democratic societies safeguard the individual's person and personality from improper police conduct such as physical brutality, compulsory self-incrimination, and unreasonable searches and seizures. As said by Professor Westin, a balance is set between "government's organizational needs for preparatory and institutional privacy and the need of the press, interest groups, and other governmental agencies for the knowledge required to keep government conduct responsible."

When we begin thinking of privacy in this larger institutional framework, we are called upon to scan the entire spectrum of surveillance technology. The pervasiveness and impact of this surveillance

---

4 The ideas contained in the next few paragraphs were derived from a reading of Westin, *Science, Privacy and Freedom: Issues and Proposals for the 1970's, Part I*, 66 COLUM. L. REV. 1003 (1966).

cannot be narrowed or isolated into one of its components, that is, data processing. Surveillance has to be considered in its totality—whether it be physical through listening or watching devices, psychological through the use of mental testing, drugs, or other emotion measuring devices, or data secured via the collection, storage, exchange and collation of comprehensive information through computers and other electronic processing systems.

We cannot overemphasize the impact of an all-embracing surveillance system on the actions of any individual or group of individuals. How would we behave in a conference room, for example, if we knew that persons were observing our every movement by some televising device? Would our freedom of speech be circumscribed if every time we made a phone call we knew some third party was listening? How would our thoughts be channeled if we knew that every fact in our lives was coded and stored in one central location, instantaneously accessible to certain persons? The potential for inhibiting our conduct, our actions and our thoughts is very real.

If we exclude the wide range of surveillance forms from our consideration, and treat the privacy issue only in relation to data processing, our efforts at resolution of the problems will be quite insufficient. Unless the issue of privacy is considered in this broader context and, as Westin states, is in the forefront of the planning and administration of future computer systems, "the possibilities of data surveillance over the individual in 1984 could be chilling."[5]

Legal Evolution of the Privacy Concept

From the legal vantage point, the concept of privacy has several facets.

One notion of privacy, evolved by the courts, is derived from a traditional common law base involving doctrines of tort, contract and property law.[6] Other courts have found a right of privacy in their respective state constitutions.[7] There also has been a judicial recognition of the right of privacy as inherent in the rights of the individual, despite the fact that it does not fit within traditional common law precepts.[8] Most significantly, recent cases decided by the United States Supreme

---

5 *Id.* at 1013.

6 Warren & Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

7 See for example Melvin v. Reid, 112 Cal. 285, 297 P. 91 (1931).

8 Pavesich v. New England Life Ins. Co., 122 Ga. 190, 50 S.E. 68 (1905).

Court have indicated that our Federal Constitution may embody a guaranty of a right to privacy.[9]

There is also a fundamental sense of the right which permeates the mind of society at large, and will naturally be reflected in a court's treatment of a privacy situation.

That the concept of privacy is not so clearly definable as the right of free speech, or freedom of religion, is evident from a study of case law and treatises. There is no clearly articulated formulation of what privacy is in fact, and we have acquired an amalgam of definitions. Privacy has been variously defined as "the right to be let alone"[10] and ". . . an interest in not having his affairs known to others. . . ."[11]

Article 17 of the United Nations' Draft Covenant of Civil and Political Rights incorporated the concept of privacy thus:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.[12]

Thus, the rubric "right of privacy" has been used in various ways to mean many things, both in law and common parlance.

The law has developed along certain lines in the privacy area, in a manner at once classical and innovative. It is classical in the sense that new ideas are superimposed upon a presently existing legal structure; for example, privacy considered as a contract right or a property right.[13] It is innovative in that, daily, the privacy concept is creatively and imaginatively dealt with by the judiciary and characterized in unique terms not describable within the ambit of well established legal jargon.

Early Cases

The judicial history of privacy began with the 1849 case of *Prince Albert v. Strange*.[14] In this case an art dealer, without authorization,

9 Griswold v. Connecticut, 381 U.S. 479, 483 (1965); *accord*, Time, Inc. v. Hill, 385 U.S. 374 (1967). However, Justice Stewart's majority opinion in *Katz v. United States*, 389 U.S. 347 (1968) indicates that the court may have some reservations about *Griswold's* holding. He implies that the States are the proper guardians of individual privacy. *Id.* at 350, n.4.

10 Roberson v. Rochester Folding Box Co., 171 N.Y. 538, 64 N.E. 442 (Ct. App. 1902).

11 RESTATEMENT OF TORTS § 867 (1939).

12 Art. 17, Draft Covenant of Civil and Political Rights, General Assembly of the United Nations, 1960.

13 Warren & Brandeis, *supra* note 6.

14 18 L. J. Ch. 120 (Mac. & G. 25 (1849)).

published for sale etchings conceived and executed by the Prince Consort. The court declared here, for the first time, that some kind of a right of privacy exists, and that it is of no consequence that such a right was not judicially recognized by the common law. The case turned not on Albert's property right in the etchings, but on the privacy accorded a Prince.

A second significant decision was the American case of *Manola v. Stevens* (unreported), involving the unauthorized photographing of an actress during her performance while scantily clad. The court here issued an injunction against publishing such photos on the ground that it was a denial of the actress' privacy and as such, denial of a property right. This case marked the derivative application of the tort-property concept of privacy: that is, the protection of the individual against the unauthorized use of some aspect of his person or some extension of his personality.

It is important to note, however, the reasoning by which the courts used to reach their end in such cases as this. They did not say, "This individual's right of privacy has been invaded and so we must stop the advertiser." Rather, they said, "The advertiser is making a profit from the use of another's name or likeness, and thus he is taking property away from one to whom it rightfully belongs." This is a far cry from affirming the existence of a right of privacy per se; it is an example of the classical method of categorizing a heretofore nonextant right into a preexisting legal doctrine.

Another important judicial analysis in this area is found in the 1905 case of *Pavesich v. New England Life Insurance Company*.[15] This case related to the unauthorized use of the plaintiff's picture for advertising purposes. Here the court openly recognized privacy as a natural right of the individual, and rejected the notion that such a right has to be superimposed on a previously existing framework such as a tort or contract. The court said:

> When the law guaranties to one the right to the enjoyment of his life, it gives him something more than the mere right to breathe and exist. While, of course, the most flagrant violation of this right would be deprivation of life, yet life itself may be spared, and the enjoyment of life entirely destroyed. An individual has a right to enjoy life in any way that may be most agreeable and pleasant to him, according to his temperament and nature, provided that in such enjoyment he does not invade the rights of his neighbor, or violate public law or policy. . . . The liberty which he derives from natural law, and which is recognized by municipal law, embraces far more than freedom from physical restraint.

15 Pavesich v. New England Life Ins. Co., 122 Ga. 190, 50 S.E. 68 (1905).

A new foundation emerged when a California state court, in *Melvin v. Reid* in 1931,[16] recognized the right on a state constitutional base. This case involved a motion picture based on plaintiff's past life as a prostitute, after she had been reformed. The court held that the state constitution, which guaranteed the individual the right to pursue happiness, was violated by this invasion into plaintiff's privacy.

Oddly enough, some of the celebrated cases in which the courts recognized a right to privacy grew out of factual situations where the court may very well have been more interested in suppressing the exhibit disclosed—e.g., photo of a scantily clad woman, a motion picture about a prostitute—than they were in safeguarding the individual's privacy. Thus a strain of puritanism in American life might, unwittingly, have had more to do with the courts' treatment of the privacy issue than the purposes which have been ascribed to it.

These cases based on the common law were not suited to deal with the technological advances of the twentieth century. While the courts were willing and able to suppress information when the person whose right was invaded was subject to loss of profits or property, they were unable to deal effectively on these terms with wiretapping, modern photography and other modern methods of surveillance which constituted a more subtle invasion of personal life.

Recent Developments

Starting in the 1950's, however, the United States Supreme Court began to find in the First, Fourth and Fifth Amendments certain aspects of what may be called a right inhering in the citizen to prevent certain governmental intrusions. Our Supreme Court, for example, has interpreted the Fourth Amendment to mean that evidence seized in contravention of the security of the individual or his home is inadmissible at trial. *Weeks v. United States*,[17] *Mapp v. Ohio*.[18]

The Supreme Court in *Watkins v. United States*,[19] recognized the individual's right to privacy by preventing a Congressional investigating committee from exposing a person's background for exposure's sake alone. While the Court recognized the right of privacy inherent in the individual, that case primarily dealt with the witness' claiming of his privilege against self-incrimination.

In *NAACP v. Alabama*,[20] the Court upheld privacy of association by refusing to order the NAACP to reveal the names of its members

16 Melvin v. Reid, 112 Cal. 285, 297 P. 91 (1931).
17 232 U.S. 383 (1914).
18 367 U.S. 643 (1961).
19 354 U.S. 178 (1957).
20 357 U.S. 449 (1958).

to the state government which ostensibly required such a list in order to admit the NAACP as an out-of-state corporation. The Court unanimously declared that privacy of association is inextricably bound up with the freedoms guaranteed in the Bill of Rights.

In *Shelton v. Tucker*,[21] teachers of Arkansas were required by the State to list every organization to which they had belonged for five years prior to their appointment. Although the Court struck down this statute as too broad in scope, it was protecting the same First Amendment right of freedom of association that it upheld in *NAACP v. Alabama.*

Commentators on cases such as *Silverman v. United States*,[22] and *Lopez v. United States*,[23] which involve electronic eavesdropping devices, indicate that the stress is on the protection of interest in privacy rather than the manner in which the interest is affected. Previously, in 1928, in *Olmstead v. United States*,[24] the Supreme Court had concluded that the Fourth Amendment did not preclude wiretapping where there was no physical invasion of the property in question.

One of the most important recent cases is *Griswold v. Connecticut*,[25] in which the majority of the Court agreed that the Connecticut contraceptive law violated the right to privacy of married persons. The Court said:

> Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."

The more recent case, *Time, Inc. v. Hill*,[26] sharply raised the issue of privacy in relation to news publications. *Life Magazine* had reported on a play which depicted the ordeal of the Hill family, which had

---

21 364 U.S. 479 (1960).
22 365 U.S. 505 (1961).
23 373 U.S. 427 (1963).
24 277 U.S. 438 (1928).
25 Griswold v. Connecticut, 381 U.S. 479 (1965).
26 Time Inc. v. Hill, 385 U.S. 374 (1967).

been held hostage by a group of escaped convicts. James Hill sued *Life* on the basis of the New York Civil Rights statute which provides that:

> A person, firm, or corporation that uses for advertising purposes, or for the purpose of trade, the name, portrait or picture of any living person without having first obtained the written consent of such person, or if a minor of his or her parent or guardian, is guilty of a misdemeanor.

James Hill asked for damages on the ground that *Life* intended to present an untrue picture in that the play represented the actual Hill family. A New York jury awarded the plaintiff a $50,000 verdict, and the defendant appealed on the ground that its right of free speech and press had been violated.

The interpretation by the New York courts of their civil rights statute was such that if the news article was true and concerned a newsworthy individual, then no action would lie. However, if the publisher should fictionalize any portion of the facts, the individual would have a cause of action against the publication. The *Life* article depicted scenes from the play which were a fictionalization of the events which actually transpired.

This case raised the issue of a clash between freedom of the press under the United States Constitution and an individual's right to privacy under a state statute. The importance of freedom of the press was emphasized in the majority opinion when Mr. Justice Brennan said, "A broadly defined freedom of the press assures the maintenance of our political system and an open society." The majority balanced this right against the individual's right to privacy and found that whenever a person becomes newsworthy or a public figure, his right to privacy must give way to the freedom of the press which protects the public's right to know. The verdict below was reversed on the narrow ground that the instructions to the jury were incorrect. The action reflected the disagreement in the Court.

Three Justices—Black, Douglas and Harlan—felt this was not a case which involved the individual's right of privacy but should be viewed strictly as a case of freedom of the press. However, it is clear from a reading of their opinions that they were concerned with the individual's right to be protected from unwarranted interference by newspapers.

The dissent of Mr. Justice Fortas, in which he was joined by Chief Justice Warren and Mr. Justice Clark, is a forthright declaration of the constitutional basis of the right of privacy. In defining this right,

Justice Fortas said: "It is, simply stated, the right to be let alone; to live one's life as one chooses, free from assault, intrusion or invasion except as they can be justified by the clear needs of community living under a government of law." His reading of *Griswold v. Connecticut,* was that it was "squarely based upon the right of privacy which the Court derived by implication from the specific guarantees of the Bill of Rights."

A Constitutional Status

Thus it is evident that some constitutional notion of a right to privacy has evolved over the years. There is a school of thought, of which Mr. Justice Black is notably one, which reads the Constitution literally and finds no basis for a right to privacy contained in it.

But Professor Beaney has noted that "it is hard to see how several of the specific rights [in the Constitution] can be given meaningful scope without necessarily safeguarding a right to privacy. It would be indeed ironic if this were not so in a constitutional system designed to protect the integrity of the individual in an age that laid stress on the necessity of recognizing both the rational and irrational elements in man but which, above all, wanted to protect his dignity and status as an individual."[27]

Parenthetically, it may be appropriate to note that in addition to the legal concept of privacy which has evolved over the years, there exists a sociological concept: that is, the things that a man *thinks* are nobody's business but his own. These things vary from era to era and from individual to individual and so are not suitable to listing. As Frank Thayer has noted:

> The right of privacy though not regularly recognized as such, has been tacitly enforced by the mores of certain peoples, good taste, and immemorial custom.[28]

Obviously, the community feeling should be part of our awareness in any discussion of the right of privacy, since in a democratic society what the public thinks its rights are is what they often become. In Professor Beaney's words: "For, at heart, the values that find expression in legal decisions, statutes, or administrative rules and orders must reflect the consensus of the leaders of opinion and action in the wider society."[29]

---

27 Beaney, *The Right to Privacy and American Law,* 31 LAW AND CONTEMP. PROB. 253, 260 (1966).

28 THAYER, LEGAL CONTROLS OF THE PRESS 434 (Foundation Press 1956).

29 Beaney, *supra* note 27 at 271.

Thus, the arrows are all aimed at the same target: that is, the point at which the Supreme Court reflects the mores of the citizens when it signals constitutional recognition of an individual's right to privacy, the right to be constitutionally free from intrusion, be it an innocuous survey or an elaborate personnel questionnaire. The judicial concern for the liberties of the individual makes it plainly visible, and it will have an immediate and dramatic effect on the future of data processing and automation in government, raising the privacy-surveillance dichotomy to a constitutional dimension.

THE BALANCE OF INTERESTS

Although a certain sanctity may protect the individual's right of privacy, that right, like so many others, is relative, even if it is to be accorded full constitutional recognition by the U.S. Supreme Court. The yardstick may well be the question: Is the information sought reasonably related to advancing the general health, welfare, or safety of the community? This is the perennial problem of balancing the citizens' interest in being left alone with society's need.

The developments of science in the last few decades would appear to have outstripped decisional law reflecting the problems and technology of the era. Today, conversations can be overheard blocks away without the persons involved ever knowing it. The computer and automated data processing equipment give the government an opportunity to process such a volume of data at such high speed that the lag between an administrative or policy decision and its effect on the citizen is tremendously reduced.

Raw data on each citizen, when placed in a computer, can be of great utility to the government. If the existence of such computerized data, however, offends the community sense of the right to privacy, and if the courts are unable to balance the competing interests to the satisfaction of the community, the reaction may be in the form of legislation not necessarily best suited to the delicate balancing required.

When we speak of the individual's right of privacy, we are essentially recognizing his right, also, to withhold certain information about himself which he may not wish to disclose. His right to withhold, however, may not be justified under all circumstances, just as the inquirer's right to know may be unwarranted in any number of situations. It is necessary to identify the competing interests in order to weigh the relative factors favoring disclosure when we focus on the data gathering stage. Here the individual's right to withhold information of a

rather impersonal, statistical nature is juxtaposed to the government's "need to know" certain information. What happens, however, when we decide to gather information of a more personal nature—on personal habits and attitudes, for example? Is not the burden on the government to justify the present need for such data?

Of course, government can resort to the answer that it is economically advantageous to collect the information now and that at some future time the information will be available for computer application when required to serve some legitimate social purpose. This approach evades the issue and generates additional problems, one of which is the potential risk of disclosure of the collected but unused information.

The situation posed is very real, and information will beget information. Furthermore, there is the rationale that this is in keeping with the continuing interest of government to know, to predict and to regulate in order to shoulder the responsibility for the well-being and affluence of its citizens. As inquiry broadens and becomes more personal, however, the question arises whether government should not be obliged to demonstrate clearly the present need for such information.

Once information is disclosed by the individual, access to it requires identification of a whole new set of competing interests. For example, should the individual himself be entitled to complete and uninhibited access to all the information the government possesses on him? Under certain circumstances, where the information, if released, might be misunderstood or harmful to the individual, access to the information may very well be denied.

Should there be free access to information on individuals as between governmental agencies on the same level, and as between federal, state and local governments? Should non-governmental inquirers—prospective employers, credit agencies, relatives, members of the press, to mention a few—have access to information on an individual?

In view of the complexities and variances involved, probably no iron-clad rule can be formulated to apply across the board to the situation in which one individual has disclosed information and he or others may seek access to it. Again, we have to resort to a balancing of competing interests. Identifying the particular interests involved, coupled with the nature of the information desired, may be crucial for the decision.

Generally, the so-called "right to know" situation arises in a context in which a third person seeks information about an individual or, perhaps, a number of individuals. This third person may be a taxpayer,

who insists on seeing the tax rolls in a community so that he can find whether the assessed valuation on his property is in line with valuations on similarly-situated properties. A newspaper reporter may want information to provide background for a story. A prospective employer has an interest in seeking to trace the work history of a job applicant. A parent may wish to be apprised of a teacher's comments on the potentialities of his child. Thus, clearly, there are legitimate areas of inquiry on the part of third persons for accessibility to information on individuals.

Oftentimes, various levels of government wish to exchange information on individuals. There may very well be wholesome reasons for such cooperative exchanges, particularly in the area of law enforcement information.

This entire matter of release of information, after an individual has made a disclosure to a governmental agency, is further complicated by the notion of consent. Does the fact that the individual has disclosed information to a specific agency for a definite purpose grant that agency *carte blanche* to revealing such information? Does not the individual reasonably anticipate that the disclosure will be kept confidential? Moreover, the legal efficacy of consent loses a good deal of its force if the individual divulged the information to secure a benefit to which he may have been entitled to under law. The contention that there has been a "consent" in this context may appear to be unrealistic. And the problem of securing an individual's consent every time the release of information is requested is a different one with which we shall have to deal.

Existing controls over the release of information secured from individuals are dealt with by legislative, judicial and executive measures. These measures vary in their import. Some demand disclosure, others prohibit it. No uniform approach is readily discernible. Consequently, the possibility of incongruous results is omnipresent. A lot of hard thinking is going to have to be exerted to devise criteria by which to measure whether disclosure is proper in a given situation.

Establishment of Safeguards

Normally, when we think of safeguards, we think in terms of those the law may provide. In the law it is an axiom that for every right infringed there exists a remedy. But invasion of one's privacy does not lend itself to a simple solution like payment of damages in a negligence case. One authority put it as follows:

> Restitution in any literal sense is simply impossible in the context of disclosures of sensitive data; once made, a disclosure cannot be erased.[30]

As such, the traditional tort money-damages approach appears ineffective in the area of privacy.

Another traditional remedy is that of injunctive relief. Again, it would appear to be of little utility in protecting an individual's right of privacy, once unauthorized access has taken place.

A deterrent to disclosure might be criminal penalties. For example, it is a crime for employees of the Internal Revenue Service to divulge information from federal income tax returns unless authorized by law. Penalties are provided for such disclosure. The Civil Rights Act also calls for criminal penalties if a community service officer discloses data learned in a conciliation conference.

Submerging all the traditional issues, however, is the threshold difficulty of discovering that an unauthorized disclosure has been made. If information was revealed, it may not be known what information was revealed, to whom it was revealed, and the extent, if any, of the harm.

Preventative Approach

Thus, a lack of weapons in the legal arsenal may very well leave those who have been wronged without a remedy in law. If this be the case, and there are strong indications that it would be, then controls of a *preventative* nature appear the way to seek to protect the right. Such an approach would at least represent a minimal effort in the right direction. In other words greater emphasis must be placed on preventing unauthorized and unwarranted access or disclosure.

It appears that this may have to be approached from two sides. On the one hand, policy-makers must determine what kind of information should be disclosed, to whom, and for what reasons. On the other hand, they must also establish controls over those in a position to make disclosures.

Data to be Disclosed

There is one broad category of data which poses no difficulty—general statistics as opposed to data on individuals. Data of this variety are, by their very nature, dehumanized and, thus, have little or no bearing on the privacy issue.

---

30 Karst, *The Files: Legal Controls over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW AND CONTEMP. PROB. 342, 351 (1966).

It is information on individuals which may require a predetermined disclosure policy. It may be established by statute that personal information gathered by a data bank may be disseminated only to governmental agencies requesting it. Furthermore, the type of data supplied to any agency might be restricted solely to that which is necessary for the function the agency is required to perform. Finally, the data might not be provided unless the agency demonstrates the need.

This selective approach is, of course, premised on the capacity of computer "hardware" to provide specific information for a specific purpose. I assume there would be no technical difficulties in this regard.

How might this work? Let us assume an individual's file is categorized to include, among other things, a criminal background. This information would be akin to what is now gathered by the F.B.I. If the F.B.I. participated in a data bank, only that information would be provided, on the basis of need, to a law enforcement agency requesting same for investigative or prosecutorial purposes.

A similar selective process might apply, for example, if a State Motor Vehicle agency wanted to determine the motor vehicle record of someone who recently moved into that state and applied for a driver's license. If all states provided such data to a central bank, the specific information sought on the individual could be rapidly ascertained.

These hypotheticals, of course, are of the simple variety. Many governmental agencies perform functions which require more personal and comprehensive information about an individual, for example, for employment purposes. Here again, an effort should be made to determine the type of information needed for a limited purpose and provided only on the basis of need. It might be necessary to require any agency wishing to participate in a data bank to determine, as a prerequisite, the kind of data it intends to retrieve. Once that determination is made and approved by a policy-making body, it would have to be adhered to stringently.

CONTROL OF DATA CUSTODIAN

The second feature of the preventative approach would involve establishing controls over the person in a position to disclose data. Assuming a predetermined policy of what, when, to whom, and for what needs information should be disclosed, the indiscretions of a data custodian may not be so difficult to minimize. But this cannot be left to the mere guidance of law itself.

Someone should be empowered to oversee the disclosure of data

in a manner consistent with legislative policy. In addition to setting forth disclosure policy, enabling legislation might set the framework of a data bank agency and provide for administrative policing of its activities.

This might take the form of a corps of custodians, certified by the State, not unlike other persons in positions of public trust who are subject to State regulation. Special training programs might be established as a prerequisite for these positions.[31] They might be private or public custodians, but, in any event, they would be divorced from the technical aspects of data systems and would be charged only with managing and controlling the flow of information to authorized recipients. Furthermore, an auditing system should be established in order that a different agency or group of individuals might, from time to time, verify the validity and handling of inquiries. In addition to auditing, this group could monitor the computer programs to insure that there are no unauthorized modes of access. Occasional attempts might be made to penetrate the system as a running check on its security.[32]

In any event, provision should be made for administrative discipline of custodians and those whom they manage. The minimum penalty for wrongful disclosure might be dismissal. It may also be appropriate to fix a statutory penalty for which the victim could sue, in addition to any actual damages which may be recoverable in a civil action.[33]

Drafting of legislation in this field is, by no means, an easy task. The office of Statistical Standards of the Budget Bureau began two years ago to draft a measure to provide specific privacy safeguards in a centralized computer system. While they agreed it should be done, it was reported that Director Raymond T. Bowman and his staff were "baffled" by the assignment.[34]

Regardless of the ultimate design of this effort, responsible State administrators and legislators cannot be any the less vigilant themselves. Anything less than a constant awareness of the potential for invasion of the citizen's privacy will be a partial abdication of our responsibility. In meeting this responsibility, it will be incumbent on us, along with others, to formulate policy as to what information should

---

31 *Id.* at 363.

32 *The President's Commission on Law Enforcement and Administration of Justice, Task Force on Science and Technology*, 75, U.S. Government Printing Office, Washington (1967).

33 Karst, *supra* note 30, at 366.

34 N.Y. Times, *supra* note 1 at 52, col. 1.

or should not be made available under a multitude of circumstances. We, and not the custodians of the information, should determine how and under what circumstances it will be made available.

The safeguards discussed herein are designed to insure that only those with a legitimate need to sensitive information may have access to it. To an extent, this is a mechanical problem, in that we must be sure that information is not inadvertently made public because a gadget went awry. Here we shall have to rely heavily on the expertise of persons qualified to gauge the risk of error and to evaluate the mechanical effectiveness of security devices. In the ultimate, however, as Professor Reich of Yale warns,

> The real protection in this area comes not from peoples' good intentions but from laws.[35]

A discussion of safeguards naturally progresses to the point where consideration of the advisability of centralizing a data system must be faced. Safeguards that may be sufficient where data are not available through a linked network of systems, or stored in a central bank, may be insufficient when centralization is the case. If we recognize the function that privacy is to fulfill in a democratic society, it may be necessary for us to insist upon the proliferation of information sources rather than run the risk of an overpowering surveillance inherent in centralization.

Vance Packard points to four major dangers of centralization: (1) computers are ill-equipped to correct errors, or allow for extenuating circumstances, for redemption is likely to be incomprehensible to a computer; (2) great power would be placed in the hands of people who would use the system; (3) public distrust of "big brother," if increased, might lead to wholesale falsification or evasion on forms; and (4) "Americans, increasingly and rightly, resent their being numbers, controlled by a computer," and they resent the accelerating depersonalization of individuals.[36]

The relationship between privacy and ADP has received some attention in prominent intergovernmental circles. In early 1968, the Committee on Information Systems of the Council of State Governments prepared a policy statement in which it was recommended that the States exercise leadership in the coordination of information systems in full consultation with local governments, and in cooperation with each other and the federal government, to achieve compatibility among the various systems. It further warned that information systems

---

35 *Id.*

36 *Id.*

should be so designed as to assure that "the privacy of individuals may not be invaded nor the confidentiality of information pertaining to persons be breached."[37]

In August of 1967, the National Association of Attorneys General also adopted a resolution pointing to the "broad legal, ethical and political ramifications" of the ADP revolution. It further urged that "the fundamental, humanistic questions, notably the issue of privacy, generated by this information be fully explored and studied" by the Committee on Information Systems of the Council of State Governments on which the National Association of Attorneys General is represented.

To be sure, a unified information system has definite economic, efficiency and spatial advantages. Sharing of facilities and time will no doubt cut operational cost. Instantaneous accessibility to a total information system will aid those who use new and unique applications to advance social objectives. These plusses cannot be discounted. Nevertheless, we are talking about a right that is precious to our political system. To the extent that we infringe upon the exercise of that right, we undermine our free society. It is, therefore, incumbent on all who are in a position to influence and initiate policy in this sphere to examine the fundamental humanistic questions occasioned by the information explosion—before these questions are completely obscured by the intricacies of the technology itself.

---

[37] *State Information Systems Policy Statement, Recommended by Committee on Information Systems of the Council of State Governments*, January 3, 1968.