Marquette Law Review

Volume 52
Issue 3 *Fall 1969*

Article 1

Centralized Information Systems and the Legal Right to Privacy

Jeffrey A. Meldman

MARQUETTE LAW REVIEW

Vol. 52 FALL, 1969 No. 3

CENTRALIZED INFORMATION SYSTEMS AND THE LEGAL RIGHT TO PRIVACY

JEFFREY A. MELDMAN*

The complexity of the policy decisions that have been explored in recent years and the increasing availability of new technologies for collecting, transmitting, and processing information have caused an increasing demand by government, university, and private sectors for more efficient access to information about multitudinous aspects of the lives of individuals. Most recently these demands have been in the form of a desire for national centers for handling such information in an orderly and comprehensive manner. Concurrent with these visions of data centers, however, considerable fear has been voiced about the threats that centralized information may pose to the sanctity and privacy of the individual. The always increasing number of files and records of personal information has been bringing more and more information about individual lives into the public light, and critics of this trend have become worried that the "Big Brother" society prophesied by George Orwell may be very close at hand.

The context of the debate about centralized data centers has focused on the conflict between two realms of value: the value of greater understanding of society and of more intelligent methods of policy formulation, and the value of allowing an individual to keep information about himself and his life private and unknown to others. But conflicts of value are neither new to the American experience, nor have they been unmanageable by the social systems and institutions that embody and structure such social values.

The legal system in America has been constantly faced with value conflicts brought about by changing technology, and it has so far shown itself to be basically well-adapted to deal with them. The legislatures, courts, and other legal and quasi-legal institutions have demonstrated considerable success in analyzing, balancing, and resolving sets of values that necessarily differ in a democratic society. The wide-felt reluctance to change values rapidly—itself a value concept—is inbred in the

* Member, Wisconsin Bar; S.B., Massachusetts Institute of Technology, 1965; LL.B., Harvard Law School, 1968.

legal process, through its doctrine of precedent and its reliance on established frames of reference in considering new proposals.

This article will explore the extent to which this legal system may be able to resolve the conflicts suggested by the establishment of centralized information systems. It will examine how the existing legal concepts of a right to privacy might be able to protect individuals from possible encroachments on their privacy by such data systems and, to the extent that present legal concepts may be inadequate, it will suggest how additional legal protection of privacy might be effected in a manner that will still allow a maximum recognition of the valuable advantages that would derive from centralization of information about individual members of the society.

THE NATURE OF THE PROPOSED SYSTEMS

Centralization of information has become a goal of persons engaged in almost every kind of activity that depends heavily on analysis of data. Data collection has tended, until recently, to operate in a piecemeal manner so that small pools of uncomprehensive data are scattered throughout the country geographically, as well as at various institutional levels. Much of this data does not relate to the circumstances of the lives of individuals. Considerable scientific and technological statistics, much medical knowledge (except for case histories), and many legal authorities are decentralized, but these are also relatively harmless to individual privacy. Standardization and centralization of this kind of data are being demanded by participants in these fields[1] without much concern by the public about possible invasions of individual privacy.

Certain demands for centralized information, however, do pertain to information about individuals. Research in the behavioral sciences, information for urban, regional, and national policy and planning, and operations of law enforcement agencies could be greatly enhanced by comprehensive personal information about each citizen. Information centers that serve these purposes are the ones that pose possible threats to the privacy of the individual, and proposals for these systems must be viewed with consideration of the privacy problem.

There are two basic kinds of data centers in this category. One is the central intelligence center that would contain complete information about each individual in the society and that would be used by law enforcement agencies and other governmental bodies to find out facts about a particular citizen under investigation.[2] The other is the central statistical center that would contain similar information, but that would be used only to find out statistical facts about groups of citizens, or populations, to aid in understanding the society, itself, and in making policy decisions in planning for the society.

[1] *See, e.g.*, TOWARD A NATIONAL INFORMATION SYSTEM (M. Rubinoff ed. 1965).
[2] Rothman, *Centralized Government Information Systems and Privacy*, TRW SYSTEMS, Sept. 22, 1966, at 1.

This article is primarily concerned with the statistical centers, for it is these centers that are currently being seriously proposed as a substantian benefit to social welfare. The intelligence systems must be briefly discussed, however, for there has been a significant tendency to confuse the two kinds of systems, and there is also considerable fear that statistical systems could be used for intelligence purposes.

Central Intelligence Systems

The characterizing feature of an intelligence data system is that its records would comprise accessible information about identified individuals. Every citizen presently generates a large number of records, public and private, as he proceeds through life, and all of these records could be combined into a centralized master file. Such centralization of birth records, census records, medical records, school records, employment records, bank records, credit bureau records, court and police records, social security records, marriage records, consumer records, tax records, military records, and others[3] would allow an investigator to acquire detailed information about a particular individual much faster and much less expensively than is now possible. Such a system would be of particular value to law enforcement agencies and other governmental bodies that rely on knowledge about individuals, and it would no doubt be of much use to private organizations such as credit bureaus and investigative agencies.

It is this system of centralized citizen dossiers that appears to conflict most squarely with notions of individual privacy. Its very purpose of providing immediate access to every last detail about a private citizen is directly opposed to the citizen's claim to privacy of personal information, and this is true whether such information would be generally available or available only to official bodies. The only advantage that these systems promise, in return for their serious encroachments upon the privacy of the lives of individuals, is a reduction of costs and delay in governmental operations.[4] The American society has always shown in its governmental structuring a strong preference for tolerating governmental inefficiency, rather than permitting the occurrence of unchecked power.[5] For this reason, perhaps, there has been little support for comprehensive systems of this kind.

Centralized Statistical Systems

Although the information contained in a statistical information center is similar to that in an intelligence center, the organization of the information and the kind of data that can be recovered from the system are considerably different. Users of a statistical system would not be

[3] P. Baran, The Data Bank v. the Individual's Right-to-Privacy, Sept. 1966, at 5 (draft for an article in DATAMATION).
[4] Rothman, *supra* note 2, at 4.
[5] Baran, *supra* note 3, at 1.

interested in the personal information pertaining to any individual citizen, but rather in the characteristic data about various populations and the correlations between these characteristics. Behavioral scientists and governmental planning bodies are interested in learning about the relationships of demographic, economic, and other social characteristics of groups of individuals, but have no interest in knowing the identity of individuals with particular characteristics, nor in knowing anything about the lives of any particular individual.

The base of information in a statistical system would comprise the same kind of assimilation of personal records that make up an intelligence system, but access to the information in the form of personal records would not be necessary. A method of retaining the identity of the individual within the system would be neceessary to permit proper matching of one set of facts about an individual with other sets of facts, so that correlations would be possible. But it would not be necessary for this identity to be accessible in any way. Procedures for insuring that these identities remain totally unknown would not in any way hamper the proper goals of users of statistical systems.

The availability of centralized information of this kind could be of considerable aid to scientific attempts to understand the dynamics of the social milieu, and to attempts by policy makers to discover more accurately the conditions and needs of the various sectors of the population and to be able to predict more accurately the effects that proposed decisions might have on these conditions and needs.

At the present time, information of a statistical nature is widely scattered among diverse governmental and private institutions throughout the country. The Bureau of the Budget, itself, lists 21 separate bureaus that provided for their own statistical program in the fiscal year 1967.[6] Much of the information is duplicate and impossible to correlate with information in other pools. Major reasons for this are: (1) the inability of separate agencies to keep track of the data collection programs of other agencies; (2) the lack of standards in classification and organization of statistics; (3) the tendencies of statistical study groups to publish only final results pertinent to a particular study and to destroy the micro-information on which these findings are based; and, (4) the immediate dissociation of the identities of individuals from their records, making impossible the later record-matching which is necessary for correlation studies. Centralized, standardized, and comprehensive records on each individual would alleviate all four of these handicaps, and the disclosure of internal identities would in no way be necessary or even desirable in such a system.

---

[6] U.S. BUREAU OF THE BUDGET, REPORT OF THE TASK FORCE ON THE STORAGE OF AND ACCESS TO GOVERNMENT STATISTICS [The "Kaysen Report"] 3 (1966).

The Proposal for a Statistical System

The major current proposal for a statistical information system originated in 1965 with a committee of the Social Science Research Council, which recommended the creation of a National Data Center.[7] This proposal was investigated and reviewed for the Office of Statistical Standards of the Bureau of the Budget by Edgar S. Dunn, Jr., in the fall of the year.[8] The Dunn Report pointed out the advantages of a centralized system, but, unfortunately, it neglected to consider the problems of privacy that might ensue from such a system.

Congressional concern as to these issues of privacy led to a series of hearings before a House Subcommittee chairmanned by Representative Cornelius E. Gallagher of New Jersey, during the summer of 1966.[9] The subcommittee heard testimony from representatives of the Bureau of the Budget, from Mr. Dunn, from computer experts, from sociologists, economists, and others, concerning the technical organization of such a center and concerning the effects that such a center might have on individual privacy. The general conclusion of Congressman Gallagher was that the present state of computer technology was inadequate to prevent the grave encroachments upon person privacy that would follow from a National Data Center, and that the value of preserving this privacy far outweighed the financial, educational, and policy-planning advantages of the system.[10]

The objections of the Gallagher Subcommittee focused on three basic areas of concern: (1) Centralized dossiers of citizens would keep an individual's past continually available to present discovery. Gallagher emphasized the Judeo-Christian concept of forgiving and forgetting a man's past and letting him make amends and begin again. The computer, Gallagher argued, cannot forget and is incapable of forgiving;[11] (2) Centralized computer files are highly vulnerable to widespread and surreptitious access. The subcommittee was particularly disturbed by the lack of legal and technological means of insuring foolproof security for the information in the system; and, (3) Systems established for purely statistical purposes are just as vulnerable and just as potentially dangerous to privacy as are intelligence systems. This conclusion derives from the necessity of retaining the identity of individuals within the system, in order that record matching be possible. The remainder of this article will investigate how these objections are expressed in the traditional

---

[7] LIBRARY OF CONGRESS, LEGISLATIVE REFERENCE SERVICE, INFORMATION CONCERNING THE PROPOSED FEDERAL DATA CENTER (Aug., 1966).

[8] U.S. BUREAU OF THE BUDGET, REVIEW OF A PROPOSAL FOR A NATIONAL DATA CENTER [The "Dunn Report"] (Dec., 1955).

[9] *Hearings on the Computer and Invasion of Privacy Before a Subcomm. of the House Comm. on Government Operations,* 89th Cong., 2d Sess. (July 26-28, 1966).

[10] 112 CONG. REC. 19,961-65 (1966) (remarks of Representative Gallagher).

[11] *Id.* at 19,962.

legal concepts of the right to privacy, how the current legal doctrines operate to protect privacy, and how further legal measures might be desirable and effective in establishing useful statistical centralization that is capable of avoiding invasions of this privacy.

The Protection of Privacy in American Law

Like the English legal system upon which it is based, American law comprises several interconnected spheres of authority. The common law formulated by the courts is an assimilation of past judicial opinions handed down in the various jurisdictions. It evolves as the courts attempt to fit the factual cases they hear into the patterns and doctrines that they have developed in previous cases. More codified legal rules exist in the form of statutes and regulations formulated by the legislatures, as representatives of the populace, and by bureaus and agencies created to administer particular realms of activity. Although the courts retain the power to interpret them, these codifications are often precipitated by the inadequacies of, or discontent with, the slowly evolving common law. Both of these legal spheres are, in turn, restricted by the mandates of the Constitution (again, subject to court interpretation), which provides the ultimate authority for the existence of the legislative, judicial, and executive powers.

The legal concept of privacy, like many legal concepts, has developed as separate doctrines in these different legal spheres. Each of these spheres must therefore be considered to understand the basic nature of privacy as it is recognized and protected by the law.

Common Law Protection of Privacy

The major realm of protection of privacy in the common law has been in the law of torts.[12] In this field, an invasion of a person's privacy is considered to be a wrong perpetrated by the invader, for which the victim can sue in a court of law for compensation. This common-law right to privacy developed mainly from the undesirable effects of two technologies quite different from the recent technology of data processing—namely from the progress in photography and newspaper publishing in the latter part of the nineteenth century. Tendencies toward yellow journalism in this period of history placed in public view intimate facts and pictures of people's lives that previously had been considered highly private matters. Individuals who were victimized by this new and widespread press coverage appealed to the courts for protection.

Prior to 1890, there were only a few courts that considered such invasions as tortious. In a case heard in 1881, a woman was allowed recovery for an intrusion, during her childbirth, of a young man pretending to be a medical assistant.[13] Several of the courts that permitted such

[12] Karst, *The Files: Legal Controls Over the Accuracy and Accessibility of Stored Personal Data,* 31 Law & Contemp. Prob. 342, 347 (1966).
[13] De May v. Roberts, 46 Mich. 160, 9 N.W. 146 (1881).

recovery did so under the doctrine that an individual had a right to be left alone. This right was not really established, however, until 1890, when Samuel Warren and Louis Brandeis published an article in the Harvard Law Review[14] strongly advocating the universal recognition of privacy as a personal right that should be protected by the courts. The authors of the article traced previous cases of recovery that were permitted under doctrines of defamation, property rights, and breach of confidence and contract, claiming that it was really privacy that the courts had been protecting. In this way, they tried to establish precedent for the doctrine and to convince the courts that a doctrine of privacy, per se, would be a more appropriate way to handle cases of disclosure of private information. The courts slowly began to follow the suggestion of this article. So many of them relied on the article for precedent that the article is often considered as having "created" the right to privacy.

As recognition of this right became more widespread, protection of privacy became divided into four basic areas:[15] (1) protection against the intrusion on the seclusion or solitude, or into the private affairs, of an individual; (2) protection against public disclosure of embarrassing private facts of an individual; (3) protection against publicity which places an individual in a false light; and, (4) protection against the appropriation of an individual's name or likeness (e.g., photograph) for monetary advantage. The first two of these areas of protection are the most relevant to the privacy problem of centralized information systems.

Protection against intrusion was at first applied only to cases of physical intrusion or physical searches of an individual's person or private property and, as such, the doctrine overlapped, to a considerable extent, the tort doctrines of trespass. Protection was then extended to cover certain kinds of sensory intrusion such as peering at individuals through windows and eavesdropping on private conversations with microphones or wiretaps. Protection against sensory intrusion was also applied to allow recovery for persistent and unwanted telephone calls to an individual.

The intrusion doctrine has also been extended to the area of personal records. In *Zimmerman v. Wilson*,[16] decided in 1936, for example, a federal court held that an unauthorized prying into the plaintiff's bank records was a tortious invasion of the plaintiff's privacy. Protection in this area, however, has not been recognized to a significant extent.

Protection against public disclosure of embarrassing private facts developed more slowly. The earliest independent application of the doctrine occurred in 1927 in *Brents v. Morgan*.[17] The defendant in this case had posted a sign in the window of his garage proclaiming that the

[14] Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
[15] Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).
[16] 81 F.2d 847 (3d Cir. 1936).
[17] 221 Ky. 765, 299 S.W. 967 (1927).

plaintiff owed him a sum of money and the court found that this public disclosure had invaded the debtor's privacy. Disclosure of embarrassing facts from an individual's past has also been protected by law. The California Court of Appeals allowed recovery in *Melvin v. Reid*,[18] in 1931, for the defendant's acts of publicizing the plaintiff's past immoral ways. The court held that all men have the right of pursuing and obtaining happiness and that the dredging up of unfavorable facts from an individual's past invades this right. This doctrine has been applied to such past facts as victimization in a robbery, indebtedness, medical history, and personal conduct.[19] Facts pertaining to sentimental associations have also been protected against public disclosure,[20] as have the contents of personal letters.[21]

At present, the majority of the states afford court protection of this kind against invasions of privacy. A minority of the states do not recognize a right to privacy in the common law, most of them allowing protection only where the invading action is proscribed by statute.[22] Over the past fifty years, however, there has been an increase in the number of states that do recognize common-law protection. That number has grown from fifteen states in 1942[23] to over thirty states at the present time.[24]

The usual form of relief granted by the courts for these invasions is an award of substantial damages. Since the nature of the tort is emotional distress rather than monetary loss, specific damages need not be alleged or proven. Nor is the difficulty in assessing the amount of the damages considered to be a bar to recovery. In addition, punitive damages may be awarded if malice on the part of the defendant can be shown. Injunctive relief, by which the court grants a request to enjoin a threatened invasion of privacy, has been rare. This is probably because the right to privacy is generally regarded as a personal right, rather than as a property right, and because most courts of equity grant injunctive relief only when property rights are involved.[25]

Legislative Protection of Privacy

Protection of the right to privacy in both state and federal statutes has been relatively spotty and non-comprehensive. Laws have been enacted partly as a response to the failure of the common law to protect rights of privacy and partly as a complement to other statutory provisions pertaining to official records. As such, the statutes rarely attempt to treat the issues of privacy in an integrated manner.

Several states have created statutes proscribing the exploitation of

[18] 112 Cal. App. 285, 297 P. 91 (1931).
[19] Prosser, *supra* note 15, at 393.
[20] 1 F. HARPER & F. JAMES, TORTS § 9.6, at 682 (1956).
[21] 41 AM. JUR. *Privacy* § 31 (1938).
[22] 77 C.J.S. *Right of Privacy* § 1(b) (1952); AM. JUR. *Privacy* § 8 (1938).
[23] Annot., 14 A.L.R.2d 750 (1950).
[24] W. PROSSER, TORTS § 112, at 831 (3d ed. 1964).
[25] 41 AM. JUR. *Privacy* §§ 34-35 (1938).

individuals' names and pictures for commercial purposes, but these laws usually comprehend the actual use of a person's name or photograph in advertising or in a commercial product such as a motion picture or novel. They do not apply to the use of private information within a commercial activity if that information is not actually publicized along with the identity of the individuals involved.

There has, however, been a relatively small amount of recent legislation aimed at curbing eavesdropping and electronic surveillance. New York, for example, proscribes the possession of devices such as "bugging" and transmitting equipment for the purpose of unconsented-to eavesdropping, as well as the use of such devices for eavesdropping on conversations in which no party has consented to the surveillance or recording. Despite these laws, however, the use, sale, and advertising of these devices is widespread throughout the state. Only two states, Maryland and Oregon, proscribe eavesdropping on conversations in which not all of the parties have given their consent.[26]

Almost all states have statutory provisions for the accessibility of official records. These provisions are usually scattered throughout the statutes, appearing in the sections of the statutes that provide for the existence of the many kinds of governmental records with which a state functions. As each governmental department or agency is created, provisions for the necessary record-gathering and bookkeeping are generally enacted at the same time. The laws pertaining to access of these records therefore widely vary among the different sets of records kept within a state. Most official records are established as "public," which usually means that anyone may have access to them, but certain more sensitive information, such as tax or health records, is defined as "confidential." Various levels of confidentiality exist. Some information may be available to any governmental body or to certain governmental bodies upon a showing of a good reason for obtaining the information, or it may be unavailable to anyone outside the original record-gathering body. Quite often, however, the accessibility of records is unclear in the statutory provisions, and questions of accessibility are left up to the discretion of the keeper of the records.[27] Regardless of the classification of the records as public or confidential, however, an individual is generally permitted to have access to his own records, and there is usually some procedure by which he can rectify errors, even if he has to resort to the courts to do it.

One of the most imaginative methods for handling accessibility of police records is a California statute pertaining to criminal prosecutions of minors. Under the California laws, a minor who is acquitted, or who serves a successful term of probation, is not only released from all pen-

[26] ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK, SPECIAL COMMITTEE ON SCIENCE AND LAW, MONITORING DEVICES AND LAWYERS number 9, at 3 (1965).
[27] Karst, *supra* note 12, at 348.

alties, but is entitled to have all records pertaining to the criminal action sealed and to have the proceedings "deemed" not to have existed. He is further entitled to answer any future questions that may be asked of him—even under oath in court—as if the proceedings had never occurred.[28] Courts, too, have been known occasionally to seal their own decisions when a release to the public would be devastating to innocent parties. The court in *United Statese v. McLeod*[29] ordered the arrests and convictions of the defendants, who were unlawfully prosecuted, to be expunged from the records.

Federal legislation has so far been even less concerned with privacy than has state law. Section 605 of the Communications Act of 1934 prohibited interception and disclosure of telephone calls, and the Supreme Court in 1937 held that this restriction applied to law enforcement agencies as well as to private individuals.[30] However, in 1941 the Attorney General ruled that section 605 would be violated by the government only if the interception and disclosure were both outside the government. This interpretation diluted the applicability of the provision considerably, and it has not been very useful in preventing wiretapping since that time.

The statutory provisions for the gathering and keeping of records within the federal government are similar to those of the states. Most federal records are public and open to universal access, but many are confidential. Confidential records may be open to certain other federal agencies, or they may be completely closed. The records of the Bureau of the Census, for example, are not accessible to any other federal agency, not even to Congress.[31]

Certain federal statutes have privacy provisions that are integral to the purposes of the acts themselves. The Civil Rights Act, for example, prohibits the gathering or disclosing of racial information in the areas in which it proscribes racial discrimination.[32]

The most far-reaching attempt so far at bringing privacy under the protection of federal legislation has been the proposed Right of Privacy Act, introduced in the Senate in February, 1967.[33] This act is aimed particularly at invasions of privacy by eavesdropping and electronic surveillance, the same problem that a few states have tried to solve with local statutes. The bill bases its authority on the commerce clause of the Constitution, claiming that wire communications are normally conducted through interstate facilities and that the manufacture, distribution, and use of eavesdropping devices are facilitated by interstate commerce. The

---

[28] *Id.*, at 366.
[29] 385 F.2d 734 (5th Cir. 1967).
[30] Nardone v. United States, 302 U.S. 379 (1937).
[31] REPORT OF THE TASK FORCE, *supra* note 6, at 7, Annex-1.
[32] Rothman, *supra* note 2, at 9.
[33] S. 928, 90th Cong., 1st Sess. (1967). The text of S. 928 is found in 113 CONG. REC. 2910-11 (1967).

act would provide for a sentence of five years and a fine of $10,000 for the willful interception or disclosure of any wire communication without the permission of at least one party to the communication. It would also provide for a sentence of one year and a fine of $25,000 for the manufacture, shipping, or advertising of any device primarily useful for interception of wire communication. For purposes of the statute, "wire communication" includes any communication made in whole or in part by aid of wire, cable, or connection, furnished or operated by any common carrier in interstate or foreign communication.

Constitutional Protection of Privacy

When the United States Constitution was framed, there was not yet any concept of a "right to privacy," as such, and the right is therefore understandably absent in the enumeration of rights guaranteed by the Constitution to every citizen. Because of the recent technological advances in eavesdropping and surveillance, however, the same concern that has led to common-law and statutory recognition of this right has also led to attempts at interpreting the Constitution in a way that affords protection from the invasion of privacy by agents of the federal government, and through the Fourteenth Amendment, from agents of state governments, as well.

The first constitutional case to face the question of governmental wiretapping was *Olmstead v. United States*,[34] decided in 1928. The police in this case used a direct wiretap to eavesdrop on the telephone conversations of the defendant. The Supreme Court held that such wiretapping did not violate any of the defendant's constitutional rights because the conversation was intangible and could not therefore be a subject of an illegal siezure prohibited by the fourth amendment. It also held that there could be no illegal search, also prohibited by the fourth amendment, since the police did not commit an actual physical trespass. Twenty-six years later, in *Irvine v. California*,[35] the court did hold police eavesdropping to be an unconstitutional search and seizure, but in this case the police had entered the defendant's home and planted microphones in the wall, as well as in the bedroom, of the defendant and his wife. Similarly, in *Silverman v. United States*,[36] in 1961, the police slipped a spike mike under the baseboard of a wall connecting the defendant's residence with a room in the adjoining building, thereby gaining contact with the heating duct in the defendant's dwelling. Again the court held that there was an unconstitutional search, only because there had been an "unauthorized physical penetration into the premises."[37] Mr. Justice Douglas based his concurring opinion on the theory that

---

[34] 277 U.S. 438 (1928).
[35] 347 U.S. 128 (1954).
[36] 365 U.S. 505 (1961).
[37] *Id.*, at 509.

what had actually been violated was the defendant's right to privacy, but the majority refused to follow this approach.

In *Lanza v. New York*,[38] the police eavesdropped on the defendant while he was conversing with his brother, a prisoner, in a prison visiting room. Once more denying the existence of a personal right to privacy, the Supreme Court held that, unlike a house or hotel room or business office, a prison visiting room was not a "constitutionally protected area."[39] These and similar cases demonstrate the court's reluctance to recognize an independent constitutional right to privacy in the area of search and seizre.

To the extent that seizable evidence is both personal and directly incriminating, however, another line of cases suggests that a right of privacy may be recognized in association with the right against self-incrimination and denial of due process. In a 1952 Supreme Court case, *Rochin v. California*,[40] three deputy sheriffs had forced their way into the defendant's room after having received "some information" that the defendant was selling narcotics. The deputies noticed two capsules lying in a night stand beside the defendant's bed, and when they called his attention to them, the defendant immediately put them into his mouth. The deputies tried forcibly to extract the capsules from his mouth, and when they failed, they handcuffed the defendant and took him to a hospital where they ordered a doctor to administer an emetic which finally caused the defendant to vomit the capsules. The capsules were found to contain morphine and were used as evidence against the defendant at his trial. The Supreme Court reversed the defendant's conviction, holding that such illegal invasion of the defendant's privacy so shocked the conscience and so offended a sense of justice that denial of due process was clear. However, in *Schmerber v. California*,[41] decided fourteen years later, the court upheld a conviction based on evidence of the alcohol content of the defendant's blood, a sample of which was taken by police order against his will. The court found no violation of the defendant's right against unreasonable search and seizure because blood tests had become so "commonplace." The court found no violation of the defendant's right against self-incrimination or a denial of due process because he was not compelled to testify against himself and because the blood test did not offend a sense of justice. The court did not mention the defendant's privacy. Why blood extraction should be considered so much less offensive than stomach-pumping is not particularly clear, but, apparently, if any right to privacy exists in this area, it is a right against shockingly offensive invasions only.

---

[38] 370 U.S. 139 (1962).
[39] *Id.*, at 142.
[40] 342 U.S. 165 (1952).
[41] 384 U.S. 757 (1966).

The first Supreme Court decision to rely directly on an independent right to privacy was *Griswold v. Connecticut*,[42] decided in 1965. In this case, the court struck down a state statute prohibiting the use of contraceptives, holding that the statute was an unconstitutional invasion of the privacy of married couples. Mr. Justice Douglas, now speaking for the majority, emphasized that many of the guarantees specifically set out in the Bill of Rights create zones of privacy that must be protected if full meaning is to be given to the enumerated rights. Mr. Justice Goldberg, in a concurring opinion, relied heavily on the ninth amendment (which provides for retention by the people of rights not specifically enumerated), in contending that the right of a married couple to privacy is a basic and fundamental personal right. Only Messrs. Justices Black and Stewart dissented, denying that there was a basis for a right to privacy in the Constitution. As a result of this case, the right to privacy finally gained clear constitutional recognition.

Legally Recognized Defenses and Justifications For Intrusions Upon the Right of Privacy

The spheres of the common law, statutory law, and constitutional law have developed several areas of protection of individual privacy. The areas of protection have been seen to be somewhat different in the various spheres. The common-law protection has been concerned chiefly with the emotional disturbance caused by intrustion into, and public disclosure of, an individual's private affairs. Privacy statutes have aimed mainly at preventing undesirable eavesdropping and surveillance. Constitutional protection, where it exists, pertains only to invasions of privacy by the government in the prosecution of criminal actions. Taken together, these measures of protection do not cover the entire realm of privacy. Even in the areas they do cover, there are numerous exceptions to the application of the protection. These exceptions illustrate how the law has had to balance the value of privacy against the values that a complete protection of privacy would attenuate, and they demonstrate how the privacy issues of centralized information centers will have to be integrated with these other social values.

Inoffensive Invasions of Privacy

In a society that is based on complex interrelations among its members, there can be no absolute right to privacy. Total privacy would imply a complete lack of contact, a "zero-relationship," with the rest of the world.[43] Only an eremite would be able to achieve such complete privacy—and few members of society would desire to live the eremite's life. Those intrusions of privacy that amount to no more than the basic activities of social intercourse must therefore be excepted from legal

[42] 381 U.S. 479 (1965).
[43] Shils, *Privacy: Its Constitution and Vicissitudes*, 31 Law & Contemp. Prob. 281 (1966).

curtailment. Accordingly, the law does not provide redress for invasions or annoyances that are reasonable, inoffensive, and unobjectionable to a reasonable man of ordinary sensitivities.[44] The courts will not allow recovery for these commonplace intrusions, statutes are rarely written to prohibit them, and, as was demonstrated by the *Schmerber* case, the Constitution has never been interpreted as proscribing them.

The standard against which offensiveness is measured is necessarily one of the current mores and standards of decency of the society at a given time. In today's world of intensive communication, most individuals do not consider telephone calls or "junk" mail or an occasional printing of their names or photographs in the newspaper as particularly offensive. *Public Utilities Commission v. Pollak*[45] is an interesting illustration of how an individual's standards of offensiveness must often give way to the community standard. The issue in this case was a commuter's complaints about the music, news, and weather reports that were played inside the public buses in which he rode to work each day. The court held for the commission, finding that the audio programs were reasonable and in the general interest of the other passengers.

Non-Public Disclosures

In order for disclosures of private information to be tortious, they must be made to the public at large, not merely to another individual. The courts have held that there is no invasion of privacy if a person tells an individual's employer about the individual's debts, or even if he tells a small group of people, unless there is a breach of confidence.[46] Under Pennsylvania law, a photograph that invades an individual's privacy is "published" each time it is shown to a third person,[47] but, in general, an invasion by disclosure must include substantial publicity.

Disclosure of Public Facts

A further exception in the protection against disclosure of personal information is made for the disclosure of "public facts"—that is, facts that are generally accessible to the public. Any personal characteristic or information that is publicly visible cannot be protected from further disclosure. When an individual goes out into a public place, he must leave many of his claims to privacy behind. Following a philosophy similar to that underlying the exception for inoffensive invasions, the courts have denied individuals the right to be alone—or unphotographed—in public.[48]

A similar distinction is made between public and private records. Governmental records that have no legislative restrictions as to access are generally considered "public," and are not protected from disclosure.

---

[44] 1 F. HARPER & F. JAMES, *supra* note 20, § 9.5, at 678; Prosser, *supra* note 15, at 396.
[45] 343 U.S. 451 (1952).
[46] Prosser, *supra* note 15, at 391.
[47] Jenkins v. Dell Publishing Co., 132 F. Supp. 556 (W.D. Pa. 1955).
[48] Prosser, *supra* note 15, at 391.

Birth records, military service records, court testimony (including pretrial hearings), and police measurements and fingerprints (if authorized) fall into this category. Government records that are in any way confidential, or that have access restrictions, are generally considered to be private, as are records kept by non-governmental concerns. Tax and census records are examples of public records that are protected from public disclosure.

Consent

One of the major defenses for the invasion of an individual's privacy is that the individual has consented to the invasion. It makes common sense, as well as legal sense, that a person should not be able to complain about an act to which he has consented, but it is not always clear when such consent exists, nor is it always simple to ascertain the extent to which a person has consented to the invasion.

Consent is a valid defense whether it is express, implied, or inferred from conduct.[49] In a society that is growing increasingly dependent upon information transfer, however, it is easy to infer consent in situations where an individual is partly coerced into giving information. An applicant for a job is expected routinely to fill out an employment questionnaire that may contain a considerable amount of sensitive information. Applicants for loans or credit are faced with similar requests. Often there are questions on such forms that are not directly relevant to the purposes of the instrument, but the applicant knows that a recalcitrant refusal to supply some of the information, because it is too personal, will meet with prompt disfavor on the part of the person who will make the job or credit decision. It is difficult to conceive of information given under these circumstances as voluntary, but consent to use information obtained in these standard ways is almost always inferred.

Legally, the consent applies only to that use of the information which was consented to.[50] The information may not be passed on to others for other uses that invade an individual's privacy. In practice, however, it is difficult to prevent this kind of traffic in personal information because of the difficulty in tracing it. The taxpayer in *Zimmerman v. Wilson*[51] was able to enjoin his bank from relaying his account information to the Internal Revenue Service, but exchanges of information usually occur without the individual's knowledge and he is usually unable to prevent it.

Need to Know

There is also a series of important justifications for invasions of privacy that have been held to outweigh the individual's right to keep personal information private. In order for society to function in an orderly manner, for example, the right of privacy is generally subject to a reason-

[49] Karst, *supra* note 12, at 344.
[50] 77 C.J.S. *Right of Privacy* § 6 (1952).
[51] 81 F.2d 847 (3d Cir. 1936).

able exercise of police power. Persons accused of crimes, whether they are later proved to be innocent or guilty, must submit to fingerprinting and photographing and other police record-taking. These records are kept available for circulation to other police agencies.[52] No question of consent is involved in such situations; rather, the necessities of proper police operations are considered to be more important than the rights of privacy.

In a similar manner, certain governmental agencies are allowed by statute, regulation, or custom to obtain records from other governmental agencies, even though some of the information may be of a confidential nature—that is, not accessible to the public. As was mentioned earlier, however, some agency records are considered too confidential for such transfer and are tightly protected.

The public's right to know about newsworthy events and people has been held as a strong justification for allowing disclosures in the press that would constitute invasions of privacy if not for their newsworthiness. This justification has been applied to cover information of an educational value to the public as well.[53]

Substantive and procedural operations of law often require disclosure of private information, and such disclosures are often allowed in the form of privileged communication. Thus, the disclosure of parties to a suit in their pleadings, and the testimony of witnesses in court and in legislatures are permitted.

There have even been cases where one party's private need to know has been held to be great enough to overshadow other individuals' right to privacy. In *Schmukler v. Ohio-Bell Telephone Co.*,[54] for example, the telephone company was permitted to monitor telephone calls in order to detect fraudulent use of its facilities.

In these exceptions and defenses and justifications for the invasion of an individual's privacy, the courts and legislatures have had to balance the value of privacy against the values of other social benefits. Sometimes the only resolution was to suspend one value in favor of another, but often the resolution attempted to maximize both as much as possible. Restrictions were usually limited to the specific areas where they were necessary, and only to the degree that was necessary. It is to be hoped that the conflicts arising from the use of centralized information can be managed in a similar manner.

Privacy In a Centralized Information System

The objections to the proposed central information system must be considered in the light of the legal doctrines of privacy. One objection to the collecting of dossier information is that it keeps personal facts

[52] Annot., 14 A.L.R.2d 750 (1950).
[53] 77 C.J.S. *Right of Privacy* § 2 (1952).
[54] 116 N.E.2d 819 (Ohio C.P. 1953).

from the past in existence. To the extent that these facts were once public, the law of privacy does not strongly recognize this objection. However, as discussed above, some courts have protected individuals from having their pasts dredged up and publicized, and this same doctrine would seem to apply to the use of past facts in an information center. The California "forgive and forget" statutes suggest further that legislative schemes for expunging might be effective in affording protection of privacy. The statutes creating a national data center, for example, might be able to provide for routine erasure of certain kinds of information after a given number of years had passed. Statutes of this kind may appear to be an Orwellian attempt at altering historical records, but the purposes here would be to protect an individual's privacy, rather than to curtail it.

Another objection to dossier files is the large probability of errors in a system that collects data about an individual from so many separate sources. Errors in identity are especially likely when a large number of similar names are assembled in one place. Use of numerical identification, such as social security numbers, has already been made by various governmental agencies as a way of successfully avoiding identification errors, however, and a continued doctrine of allowing an individual to gain acceess to his own file, for monitoring and correcting, would provide a further check on errors.

Furthermore, the objections raised to the dossier systems do not apply to purely statistical systems. Dunn emphasized, in defense of his original report, that he was considering only the statistical systems and that in such systems there was never any disclosure of personal information or identity.[55] Continued existence of past records and errors in individual records are no threat to privacy as long as the information is secure.

The other objections to a centralized system pertain to the ease with which access to the information can be gained and to the danger of surreptitious use of even a statistical system for intelligence purposes. It is in these areas that the systems pose the largest threat to individual privacy.

The laws of privacy as they presently exist might be able to protect against some of these threats. Constitutional protection against illegal search and seizure may be adequate to keep law enforcement agencies out of the system, unless they could first meet the stringent requirements of obtaining an appropriate search warrant. The mere existence of centralized information provides no reason for the FBI or the CIA to automatically have access to it. Statutory prohibition against interception of

---

[55] Address ["The Idea of a National Data Center and the Issue of Personal Privacy"], MENSA meeting, October 21, 1966.

communications, such as that proposed by the Right of Privacy Bill, might equally prohibit tapping of inter-computer information transfer.

The common-law doctrines of privacy might also afford a degree of protection. Widespread access to centralized information implies possible disclosure to a great number of people, and disclosure of information through the system might well be considered sufficient to establish the legal requirement of public disclosure. The doctrine of intrusion, which prevented the release of bank records in the *Zimmerman* case, might well be extended to cover release of records in a centralized data center.

Certain aspects of the centralized systems, however, might tend to curtail relief in the courts. The obtaining of information from the system may become so commonplace, for example, that the courts might consider such intrusions as inoffensive to the reasonable man. The "need to know" justification may also become more extensive as the increased availability of information causes increased pressure for the obtaining of such information.[56] More and more information might come to be considered public because of its existence in a national record file, and this information might thus become more vulnerable to disclosure. There may be stronger and stronger coercion to "consent" to giving personal information as the number of agencies that use the information grows, and the consent that is given may be deemed to apply to wider and wider uses of the information, since the individual will be more aware of the many users of the system.

The common law may be able to develop other lines of attack to protect information. Alan Westin suggests the recognition of privacy or "personality" as a property right so that it can be afforded greater protection.[57] The law of negligence might be extended into the maintenance of the information system, to insure a higher degree of care in handling the information.

On the whole, however, common-law notions of privacy are aimed too acutely at protection of undue publicity and emotional distress to meet the problems of privacy in a centralized information system. Nor are suits at law a particularly effective means of affording relief to those whose privacy might be invaded by the system. Suits would be expensive and time-consuming, and they would be especially burdensome upon the courts if enough of the millions of potential plaintiffs found reason to sue. Direct evidence of the invasion would probably be very difficult to obtain, and even where plaintiffs were successful, monetary compensation would usually be inappropriate to the nature of the wrong that they had suffered.

Legislation specifically relevant to the organization of the proposed information center would appear to be a more appropriate legal solution.

[56] Michael, *Speculations on the Relation of the Computer to Individual Freedom and the Right to Privacy*, 33 GEO. WASH. L. REV. 270, 277 (1964).
[57] A. WESTIN, PRIVACY AND FREEDOM 325 (1967).

With so many forms of interrelated access possible, careful legislation would be needed to explicate precisely who is entitled to have access to what. Criminal sanctions for misbehavior would provide a much stronger deterrence than would the vague fear of a possible lawsuit. In a 1966 review of the Dunn Report, a Budget Bureau Task Force Committee headed by Carl Kaysen suggested how the internal organization of a data center might also provide for a high degree of confidentiality.[58] Accompanying the creation of statutory and organizational protection of information in the central system, however, there might have to be appropriate relaxation of the present security restrictions in the agencies from which the centralized data is gathered.[59] Considerable care would have to be taken to insure against legal loopholes in the security of the system as a whole.

Even with a comprehensive statutory protection of security, though, there still exists considerable concern that enforcement of security measures would be difficult, if not impossible, because of great temptation and ease of access.

It is widely believed that access to a central computerized store of information is much easier and much cheaper than is access to the various decentralized manual records that now exist throughout the country.[60] This would supposedly provide a stronger incentive than now exists for illicit probes into private files for purposes of detection and blackmail by individual criminals as well as by members of organized crime syndicates. Critics of this position claim that manual probes are just as easy as centralized probing would be, due to the rather slipshod security habits that exist for physical records.[61] Students in a current seminar at the Massachusetts Institute of Technology, who have been testing the effectiveness of security measures at their own school, have generally had more difficulty in obtaining information from computer records than from manual files, and many of these students are themselves knowledgable in computer technology.

The efforts of the computer industry to provide for security technology have thus far been minimal, but the potential for protection circuitry is high. Proposed methods for protecting computer records from surreptitious access include: cryptography in transmission of data; scrambled storage formats; random external auditing of record use and program alterations; isolation of the user from all programs; isolation of programmers from real data; automatic recording of users' identity and of the resulting disclosures; detection of abnormal requests; anti-intelligence-format programming; multi-leveled privileged modes of operation; carefully followed user identification and authentication

[58] REPORT OF THE TASK FORCE, *supra* note 6.
[59] REVIEW OF A PROPOSAL, *supra* note 8, at 35.
[60] P. BARAN, COMMUNICATIONS, COMPUTERS AND PEOPLE 11 (1965).
[61] Rothman, *supra* note 2, at 1.

procedures; restricted physical access to files and hardware; and, of course, carefully chosen personnel. The most effective way to prevent intelligence use of a statistical system would be to use code identities within the active system and to keep the keys to these codes—and therefore the information necessary to learn identities—totally inaccessible except at certain times and to certain personnel, and then only upon multiple signatures or keys.[62]

The systems could not be foolproof, but few social dangers can be eliminated completely. Banking has not been abandoned simply because bank robbery can not be totally curtailed. What is necessary is that the risks of the system be reduced to a low enough level so that the advantages of the system outweigh them. The same computer technology that created the current widespread use of information appears to be fully capable of protecting that information to a significant degree. At the very least, it would seem able to make illegal access to centralized information more difficult and more expensive than access to information available elsewhere.

Technological security, although possible, must be paid for. There has so far been no profit motive within the computer industry for security systems, and it is unlikely that internal competition will generate much interest in developing this phase of the technology. As the computer becomes used more and more in privacy-sensitive areas, however, the industry will be forced to realize that it is marketing a potentially dangerous product. Like any other manufacturer of dangerous merchandise, the computer industry will be expected to take the responsibility for providing the necessary safety features. This responsibility has generally been considered the price that a maker of a dangerous product must pay for the privilege of selling the product to the public.[63] Industries that have attempted to shirk this responsibility have usually found themselves subject to legislative regulation, as the example of the automobile industry demonstrates. However, whether technological security measures are generated from within the industry or imposed by law, these safeguards will in all probability protect individual privacy in a centralized statistical information center to considerable extent.

It would thus appear likely that legal and technological arrangements are capable of protecting privacy in the proposed systems for national statistical information. If arrangements of this kind are in fact achieved, the conflict between the value of intelligent policy planning and the value of personal privacy can be resolved without a significant sacrifice in either value.

---

[62] Ruebhausen & Brim, *Privacy and Behaviorial Research*, 65 COLUM. L. REV. 1184, 1205 (1965).
[63] BARAN, *supra* note 60, at 16.