1978

Toward a Comprehensive Fair Information Standards Law: A Commentary on the Data Privacy Issue in Minnesota

G.Theodore Mitau

Toward a Comprehensive Fair Information Standards Law: A Commentary on the Data Privacy Issue in Minnesota

G. Theodore Mitau*

The relationship between the collection and use of information by the government and a possible zone of personal privacy has become a pressing political and legal issue in this country. The real and potential danger inherent in widespread governmental use of computer technology demands a careful and continuing analysis of the conflict between the perceived needs of administrators and the reasonable expectations of personal privacy. In order to avoid unintended consequences that significantly shift risks, rights, and duties between government and individual citizens, strict constraints must be imposed to limit the manner in which governmental agencies gather, use, and disclose personal information.

I. THE MAGNITUDE OF THE PROBLEM

In recent years, the data collection and retention capabilities of the government have rapidly expanded as a result of technological improvements in data processing and an overall increase in the number of computers available.[1] One indication of this expansion is the federal government's inventory level of automatic data processing equipment, which rose from a mere two computers in 1951 to a total of nearly six thousand in 1971.[2] By utilizing these enhanced data processing capabilities, federal agencies can now have access to significant amounts of personally intrusive information concerning vast numbers of people. For example, the United States Civil Service Commission has a security investigation index containing over ten million index cards,[3] the Washington National Records Center main-

* Distinguished Service Professor of Political Science, State University System of Minnesota. The research assistance of Frederick D. Huebner and Robert W. Sargeant is gratefully acknowledged.

1. *See* PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY app. 5, at 10-15 (1977) (Technology and Privacy).

2. *See* U.S. GENERAL SERVICES ADMIN., AUTOMATIC DATA PROCESSING EQUIPMENT INVENTORY 18, chart 1 (1977); Ervin, *The First Amendment: A Living Thought in the Computer Age*, in SURVEILLANCE, DATAVEILLANCE AND PERSONAL FREEDOMS 24 (1973) (original version appeared in 4 COLUM. HUMAN RIGHTS L. REV. 1-235 (1972)) (citing U.S. GENERAL SERVICES ADMIN., INVENTORY OF AUTOMATIC DATA PROCESSING EQUIPMENT IN THE UNITED STATES FISCAL YEAR 1971, at 15).

3. Ervin, *supra* note 2, at 31.

tains over two million investigative files,[4] and the investigative records of the United States Army contain seven million files "relating principally to security and criminal investigations of former and present members of the Army, civilian employees, and employees of private contractors doing business with the Army."[5]

State and local governments have also expanded their computer and informational capabilities. A 1970 report by the National Association for State Information Systems indicated that 35 states employed over 24,500 people to maintain and develop automatic or electronic data processing systems.[6] During the five-year period from 1966 to 1970, the computer capabilities of state governments increased by fifty percent.[7]

As the need for more comprehensive governmental services and regulatory activities increases, demand for information will undoubtedly escalate, perhaps exponentially. Public agencies facing legislative insistence on greater accountability, more effective management practices, and more elaborate budget justifications will search for broader informational resources with which to make decisions. In such a context, computer-based information systems offer an enormous potential for data storage and retrieval that will no doubt prove useful. Policy questions concerning education, taxation, law enforcement, welfare, health care, employment, energy, and the environment often require an immense data base for impact studies and simulation models. Effective scientific analysis and evaluation of policy consequences in these areas demand extensive data files of group, family, and individual characteristics.

Although the demand for information may be great, it is difficult to overstate the threat these developments pose for individual privacy. For example, testimony received by the Senate Select Commit-

4. *Id.*

5. *Id.* at 33. Additional information about millions of citizens is stored in the files of such diverse federal agencies and departments as the Veterans Administration, the Census Bureau, the Internal Revenue Service, the Federal Election Commission, the Defense Intelligence Agency, the Federal Communications Commission, the Justice Department, the Securities and Exchange Commission, the Treasury Department, and the Small Business Administration.

6. *Id.* (citing NATIONAL ASSOCIATION FOR STATE INFORMATION SYSTEMS, INFORMATION SYSTEMS TECHNOLOGY IN STATE GOVERNMENT 18 (1970)).

Private business and commercial use of automatic data processing in credit information service has reached an equally impressive volume. For example, Sears Roebuck & Co. reportedly maintains 24 million active credit accounts; Equifax, Inc., an Atlanta credit reporting company, prepares up to 35 million reports a year, including more than sixty percent of all insurance investigations. BUS. WEEK, April 4, 1977, at 104.

7. NATIONAL ACADEMY OF SCIENCES, DATABANKS IN A FREE SOCIETY 64 (A. Westin & M. Baker eds. 1972) (citing NATIONAL ASSOCIATION FOR STATE INFORMATION SYSTEMS, INFORMATION SYSTEMS TECHNOLOGY IN STATE GOVERNMENT (1970)).

tee to Study Governmental Operations led the Committee to conclude that "domestic intelligence activity has threatened and undermined the constitutional rights of Americans to free speech, association and privacy."[8] The Committee found that domestic intelligence operations, conducted under claimed inherent executive powers,[9] subjected a wide range of individuals, from political activists to governmental employees and elected officials, to "[s]urreptitious entries . . . in violation of law"[10] and to covert tactics aimed at discrediting their reputations, disrupting their careers, and destroying their marriages.[11] The Nixon impeachment hearings document the lengths to which former President Nixon went in employing governmental agencies and data processing capabilities for constitutionally questionable purposes.[12]

---

8. SENATE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, Book II, S. REP. No. 755, 94th Cong., 2d Sess. 290 (1976). In addition to finding that "intelligence agencies . . . regularly collected information about personal and political activities irrelevant to any legitimate governmental interest," *id.* at 165, the Committee concluded that

> (a) Large numbers of law-abiding Americans and lawful domestic groups have been subjected to extensive intelligence investigation and surveillance.
>
> (b) The absence of precise standards for intelligence investigations . . . contributed to overbreadth . . . .
>
> (c) The intelligence agencies themselves used imprecise and overinclusive criteria in their conduct of intelligence investigations . . . extend[ing] beyond "subversive" or violent targets to additional groups and individuals subject to minimal "subversive influence" or having little or no "potential" for violence.
>
> (d) Intelligence agencies pursued a "vacuum cleaner" approach to intelligence collection—drawing in all available information about groups and individuals, including their lawful political activity and details of their personal lives.

Id.

9. *Id.* at 134.

10. *Id.* at 204.

11. *Id.* at 211. Perhaps the most notorious example of such activities was the campaign to "neutralize" Dr. Martin Luther King, Jr. Intelligence operations included microphones planted in his bedroom, physical and photographic surveillances, and anonymous mailings. One mailing included a tape with an unsigned letter, sent just prior to Dr. King's departure for Europe where he was to receive the Nobel Peace Prize, that warned him, "'your end is approaching . . . you are finished.'" *Id.* at 221. Additional efforts to destroy Dr. King and his movement led the FBI to engage in measures that would "prevent him from meeting with world leaders, receiving honors or favorable publicity, and gaining financial support." *Id.* at 222.

In other intelligence operations, various governmental agencies opened and photographed nearly 250,000 pieces of first-class mail, intercepted millions of private telegrams, and established over 500,000 domestic intelligence files on various individuals and groups. *See id.* at 6-7.

12. Article II of the Articles of Impeachment adopted by the House Judiciary Committee illustrates how President Nixon allegedly misused government data banks:

The familiar warning that "it will go on your records and follow you the rest of your life" takes on new meaning as governmental agencies adopt state-of-the-art computer technology. Cases documenting actual agency abuse of sensitive data abound,[13] but even

(1) He has, acting personally and through his subordinates and agents, endeavored to obtain from the Internal Revenue Service, in violation of the constitutional rights of citizens, confidential information contained in income tax returns for purposes not authorized by law, and to cause, in violation of the constitutional rights of citizens, income tax audits or other income tax investigations to be initiated or conducted in a discriminatory manner.

(2) He misused the Federal Bureau of Investigation, the Secret Service, and other executive personnel in violation or disregard of the constitutional rights of citizens, by directing or authorizing such agenies or personnel to conduct or continue electronic surveillance or other investigations for purposes unrelated to national security, the enforcement of laws, or any other lawful function of his office; . . . and he did direct the concealment of certain records made by the Federal Bureau of Investigation of electronic surveillance.

(3) He has, acting personally and through his subordinates and agents, in violation or disregard of the constitutional rights of citizens, authorized and permitted to be maintained a secret investigative unit within the office of the President . . . .

Articles of Impeachment, H.R. REP. No. 1305, 93d Cong., 2d Sess., 120 CONG. REC. 29219 (1974).

13. An alarming example of misuse of sensitive information occurred recently in Minnesota. A child in a suburban elementary school was placed in a program for retarded children. When her parents learned of this, they took the child to the University of Minnesota for evaluation. The University psychologist determined that the child was not retarded but did have a learning disability related to a hearing problem. When these results were transmitted to the school, the child was placed in the proper program. The parents, concerned that the "retarded" label may become known and cause the child problems in the future, requested that the inaccurate data be changed to reflect the child's true mental condition. The school district, while admitting that the "retarded" label was incorrect, refused to change the school records. *See* Memorandum from Donald Gemberling, Minn. Dep't of Administration, Data Privacy Unit, to Representative Shirley Hokanson (Apr. 20, 1977).

State *ex rel.* Tarver v. Smith, 78 Wash. 2d 152, 470 P.2d 172, *cert. denied*, 402 U.S. 1000 (1970), presents another startling illustration of what may happen to a data subject in a welfare setting. Catherine Tarver, a welfare mother with three minor children, became ill and was hospitalized. Local police placed her children in the county youth center, under the care and protection of the juvenile court. After reviewing an unsubstantiated report by her caseworker alleging child neglect, the court removed the children from Ms. Tarver's custody. Although she was later exonerated and the children returned to her custody, the caseworker's report remained in Catherine Tarver's file at the Washington Department of Public Assistance. Ms. Tarver wanted to have the report removed from her file on the grounds that it was false, misleading, and prejudicial. When she requested that the Department hold a hearing in which she might challenge the report, the Department refused, arguing that the grievance was not directly related to eligiblity for public assistance. The state court agreed with the welfare agency. Catherine Tarver's file remains intact.

these do not accurately reflect the magnitude of the problem. As one commentator noted, "[w]e must recognize that we are dealing with a new technology, whose applications are just beginning to be perceived and whose capacity to deprive us of our privacy simply cannot be measured in terms of existing systems or assumptions about the immutability of the technology."[14]

This Article will examine several possible ways of dealing with the data privacy issue. It will suggest that currently neither the United States Constitution nor state constitutions are sufficient to ensure an effective zone of personal privacy in informational concerns. Following an examination of the Minnesota Data Privacy Act, the Article will delineate several specific deficiencies of this statutory approach and will suggest how these problems might best be solved.

II. A CONSTITUTIONAL RIGHT OF PRIVACY

The United States Supreme Court has recognized that certain individual privacy interests are constitutionally protected, guaranteeing to individuals the freedom to make decisions regarding the intimate and fundamental areas of their lives.[15] This aspect of per-

14. Miller, *Symposium—Computers, Data Banks, and Individual Privacy: On Proposals and Requirements for Solutions*, 53 MINN. L. REV. 224, 227 (1968).

15. In Griswold v. Connecticut, 381 U.S. 479 (1965), Justice Douglas, writing for the majority, found a Connecticut statute outlawing birth control devices to be an unwarranted intrusion into the "sacred precincts of marital bedrooms." *Id.* at 485. In a remarkably creative piece of constitutional interpretation, the statute was held to contravene a "zone of privacy"—a "penumbral" right created by, but not contained in, the various textual guarantees of the first, third, fourth, fifth, ninth, and fourteenth amendments. *See id.*

The constitutional basis for a right of personal privacy was developed further in Roe v. Wade, 410 U.S. 113 (1973). In the majority opinion, Justice Blackmun expressed puzzlement over the source of a right of privacy, but determined that, wherever the right came from, it was "broad enough to encompass a woman's decision whether or not to terminate her pregnancy." *Id.* at 153. Apparently reluctant to rely too heavily on the precarious penumbra doctrine of *Griswold,* Blackmun found traces of a right of privacy in cases that had held constitutionally protected the private possession of obscene material, *see* Stanley v. Georgia, 394 U.S. 557 (1969), a phone conversation in a public phone booth, *see* Katz v. United States, 389 U.S. 347 (1967), various aspects of the marriage relationship, *see* Loving v. Virginia, 388 U.S. 1 (1967), the use of contraceptives, *see* Eisenstadt v. Baird, 405 U.S. 438 (1972), and the rearing and education of one's children, *see* Pierce v. Society of Sisters, 268 U.S. 519 (1925). The contribution of the *Roe* Court is its suggestion that the constitutional guarantee of personal privacy might protect other interests "that can be deemed 'fundamental' or 'implicit in the concept of ordered liberty.' " 410 U.S. at 152 (quoting Palko v. Connecticut, 302 U.S. 319, 325 (1937)).

sonal privacy, which might be termed "autonomy,"[16] should be distinguished from "informational privacy,"[17] which appears to be a triangular configuration composed of the individual, the government, and one or more third parties. An individual's interest in informational privacy encompasses not only the manner in which the state gathers and uses personal information,[18] but also the impact that disclosure of such information to third parties will have upon the data subject.[19]

It is doubtful that the Federal Constitution will be fully able to guarantee emerging expectations of informational privacy against an increasingly inquisitive bureaucracy seeking data to fill its vast computer memory banks. In *Paul v. Davis*,[20] for example, the Supreme Court refused to extend to informational privacy the constitutional protections that it had previously extended to personal autonomy. The Court held that a person who had been arrested for, but not convicted of, shoplifting could not assert a constitutional right of privacy against police publication of his name and picture as a "known" thief.[21] *Paul* is particularly relevant to data privacy concerns since the Court expressly stated that the publication of deroga-

16. *See generally* Henkin, *Privacy and Autonomy*, 74 COLUM. L. REV. 1410 (1974).

17. *See* Whalen v. Roe, 429 U.S. 589, 598-99 & n.24 (1977).

18. Olmstead v. United States, 277 U.S. 438 (1928), presents one example of how the government has used developing technology for the purpose of gathering information. Although the majority in *Olmstead* held that evidence procured by a warrantless wiretap of a defendant's private phone conversation was admissible, the case is best remembered for the dissenting opinion of Justice Brandeis, who argued for a broad right of personal privacy. Brandeis characterized the right of privacy as "the right to be left alone—the most comprehensive of rights and the right most valued by civilized men." *Id.* at 478. The dissent, which suggested a fourth amendment foundation for the right of privacy, was reminiscent of an earlier work in which Brandeis had expressed a prophetic concern about the "numerous mechanical devices that threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the housetops.'" Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

Although Katz v. United States, 389 U.S. 347 (1967), subsequently overruled *Olmstead*, the Supreme Court was not willing to adopt fully the suggestion of Justice Brandeis:

> [T]he Fourth Amendment cannot be translated into a general constitutional "right to privacy." That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all. Other provisions of the Constitution protect personal privacy from other forms of governmental invasion. But the protection of a person's *general* right to privacy—his right to be let alone by other people—is, like the protection of his property and of his very life, left largely to the law of the individual States.

Id. at 350-51 (footnotes omitted).

19. *See generally* A. WESTIN, PRIVACY AND FREEDOM 158-68 (1967).

20. 424 U.S. 693 (1976).

21. *See id.* at 713.

tory information from an official record did not contravene the plaintiff's constitutional right of privacy:

> Respondent's claim is far afield from [the personal autonomy] line of decisions. He claims constitutional protection against the disclosure of the fact of his arrest on a shoplifting charge. His claim is based, not upon any challenge to the State's ability to restrict his freedom of action in a sphere contended to be "private," but instead on a claim that the State may not publicize a record of an official act such as an arrest. None of our substantive privacy decisions hold anything like this, and we decline to enlarge them in this manner.[22]

Put simply, *Paul* determined that while the Constitution provides some protection for personal autonomy, it does nothing to ensure informational privacy.

In *Whalen v. Roe,*[23] the Supreme Court had occasion to reconsider whether the Constitution limits how a state can gather and use personal information. Responding to a concern that potentially harmful drugs were being prescribed and dispensed illegally, the New York Legislature enacted a statutory program requiring all prescriptions for certain drugs to be recorded.[24] The name, address, and age of the patient, along with the type and dosage of the drug, were filed in computer data banks. A group of patients who had been regularly receiving such drugs commenced an action challenging the constitutionality of the patient identification requirement. The plaintiffs alleged that persons in need of the restricted drugs would decline treatment because of their fear that governmental misuse of the sensitive data would "cause them to be stigmatized as 'drug addicts.' "[25]

The district court held that the doctor-patient relationship was "one of the zones of privacy accorded constitutional protection"[26] and enjoined enforcement of the statute.[27] The Supreme Court reversed on the ground that the statute adequately protected the privacy concerns raised by the plaintiffs.[28] Notwithstanding clear language to the contrary in *Paul,* the Court's discussion seemed to imply that some aspects of informational privacy may be constitutionally protected:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the

22. *Id.*

23. 429 U.S. 589 (1977).

24. N.Y. PUB. HEALTH LAW §§ 3331(6), 3332(2)(a), 3334(4) (McKinney 1977).

25. 429 U.S. at 595.

26. Roe v. Ingraham, 403 F. Supp. 931, 936 (S.D.N.Y. 1975), *rev'd sub nom.* Whalen v. Roe, 429 U.S. 589 (1977).

27. *See id.* at 938.

28. 429 U.S. at 605.

> distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces and the enforcement of the criminal laws, all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty originally has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data—whether intentional or unintentional—or by a system that did not contain comparable security provisions.[29]

Although *Whalen* suggested that some informational privacy concerns may be constitutionally protected, it did not attempt to delineate the boundaries of that protection. Thus, especially when considered in light of the *Paul* decision, *Whalen* does not go very far toward vindicating reasonable expectations of informational privacy. While the case leaves room for further development of the right of privacy in the context of proliferating state use of computer technology, it simply cannot be relied on to prohibit all potential abuses of personal data by governmental agencies.

It may also be unrealistic to expect a majority of the present Supreme Court enthusiastically to endorse an expansive construction of the elusive constitutional right of privacy. Indeed, disappointment with the Burger Court's consistent refusal to take an active role in protecting civil liberties generally led Justice Brennan recently to invite state supreme courts to interpret their own constitutions broadly in order to guarantee individual rights and liberties:

> If the Supreme Court insists on limiting the content of due process to the rights created by state law, state courts can breathe new life into the federal due process clause by interpreting their common law, statutes and constitutions to guarantee a "property" and "liberty" that even the federal courts must protect.[30]

Justice Brennan praises various state court decisions imposing higher standards of civil liberties than would have been required by the present majority of the Supreme Court.[31] The California Supreme

29. *Id.* at 605-06 (footnote omitted).

30. Brennan, *State Constitutions and Protection of Individual Civil Rights,* 90 HARV. L. REV. 489, 503 (1977) (footnote omitted).

31. *See id.* at 498-502. Justice Brennan cites, for example, a New Jersey case that went beyond Schneckloth v. Bustamonte, 412 U.S. 218 (1973), and imposed a higher

Court, for example, in insisting on strict adherence to *Miranda v. Arizona*,[32] said,

> [W]e . . . declare that *Harris* [*v. New York*] is not persuasive authority in any state prosecution in California.
>
> . . . .
>
> We pause . . . to reaffirm the independent nature of the California Constitution and our responsibility to separately define and protect the rights of California citizens despite conflicting decisions of the United States Supreme Court interpreting the federal Constitution.[33]

Justice Brennan suggests that such developments illustrate one of the great strengths of our federal system: "[I]t provides a double source of protection for the rights of our citizens."[34] To the extent that state courts heed Brennan's call to "thrust themselves into a position of prominence in the struggle to protect the people of our nation from governmental intrusions on their freedoms,"[35] the right of privacy may find more protection in state constitutions than the Supreme Court has allowed it under the Federal Constitution.

If a state constitution does not expressly refer to a right of privacy, state courts are left to discover guarantees of privacy in the interstices of the constitutional text.[36] Although several state constitutions explicitly guarantee a right of personal privacy,[37] the mere

---

fourth amendment standard, *see* State v. Johnson, 68 N.J. 349, 346 A.2d 66 (1975); cases from California and Hawaii that demand a standard of reasonableness, rather than automatic validation, for searches incident to lawful arrest, *compare* People v. Brisedine, 13 Cal. 3d 528, 531 P.2d 1099, 119 Cal. Rptr. 315 (1975), *and* State v. Kaluna, 55 Haw. 361, 520 P.2d 51 (1974), *with* United States v. Robinson, 414 U.S. 218 (1973); a Michigan case that entitles suspects to the assistance of counsel when a photographic identification procedure is used, *compare* People v. Jackson, 391 Mich. 323, 217 N.W.2d 22 (1974), *with* United States v. Ash, 413 U.S. 300 (1973); and cases that establish a right to trial by jury even for petty offenses, *see* State v. Sklar, 317 A.2d 160 (Me. 1974); Parham v. Municipal Court, 199 N.W.2d 501 (S.D. 1972).

32. 384 U.S. 436 (1966).

33. People v. Disbrow, 16 Cal. 3d 101, 113, 114-15, 545 P.2d 272, 280, 127 Cal. Rptr. 360, 368 (1976) (footnotes omitted). In Harris v. New York, 401 U.S. 222 (1971), the Supreme Court held that statements inadmissible in the prosecution's case in chief because not obtained in accordance with the procedural safeguards imposed by *Miranda* were nevertheless admissible for impeachment.

34. Brennan, *supra* note 30, at 503.

35. *Id.*

36. *See, e.g., In re* Quinlan, 70 N.J. 10, 40, 355 A.2d 647, 663 (1976). The New Jersey Supreme Court, citing Griswold v. Connecticut, 381 U.S. 479, 484 (1965), and Roe v. Wade, 410 U.S. 113, 153 (1973), found a right of privacy in the New Jersey Constitution: "All persons are by nature free and independent, and have certain natural and unalienable rights, among which are those of enjoying and defending life and liberty, of acquiring, possessing, and protecting property, and of pursuing and obtaining safety and happiness." N.J. CONST. art. 1, ¶ 1.

37. "The right of the people to privacy is recognized and shall not be infringed

inclusion of a privacy article in a state constitution has not always persuaded state courts to give explicit judicial sanction to significantly enlarged or consistently applied guarantees of individual autonomy.[38] Furthermore, no state constitution makes the conceptual distinction between autonomy and informational privacy. Likewise, no state constitution appears to impose any positive duty upon state government to exercise care or watchfulness in information collection, maintenance, and dissemination.[39]

. . . ." ALAS. CONST. art. I, § 22.

"No person shall be disturbed in his private affairs, or his home invaded, without authority of law." ARIZ. CONST. art. II, § 8.

"All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." CAL. CONST. art. I, § 1.

"The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches, seizures, and invasions of privacy shall not be violated . . . ." HAWAII CONST. art. I, § 5.

"The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means . . . ." ILL. CONST. art. I, § 6.

"*Right to Privacy:* Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy . . . ." LA. CONST. art. I, § 5.

"The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest." MONT. CONST. art. II, § 10.

"The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated . . . ." S.C. CONST. art. I, § 10.

"No person shall be disturbed in his private affairs, or his home invaded, without authority of law." WASH. CONST. art. I, § 7.

38. For example, courts applying state constitutional privacy provisions have nevertheless held that intrusive antiabortion statutes were not violative of privacy, *see* State v. Campbell, 263 La. 1058, 270 So. 2d 506 (1973), and that "no constitutional right of privacy . . . encompasses the right to use and possess marijuana [within one's home]," State v. Anderson, 16 Wash. App. 553, 558 P.2d 307, 309 (1976).

39. "Illinois is . . . the only state whose constitution explicitly guarantees an affirmative legal remedy for privacy invasions [ILL. CONST. art I, § 12]. So far, however, the Illinois courts have not been asked to decide whether the State constitutional right extends to records a private-sector record keeper maintains about an individual." PRIVACY PROTECTION STUDY COMMISSION, *supra* note 1, app. 1, at 1 (Privacy Law in the States).

None of the nine state constitutional privacy articles, the texts of which appear at note 37 *supra*, explicitly refers to the concept of informational privacy. Recently, however, a California court of appeals held that the constitutional right of privacy extended to the disclosure of personal information. *See* Porten v. University of San Francisco, 64 Cal. App. 3d 825, 134 Cal. Rptr. 839 (1976).

This is not to say that a constitutional approach to data privacy is fundamentally misconceived. A carefully drafted state constitutional amendment would provide an authoritative and permanent guide for those courts that are otherwise hesitant to protect reasonable expectations of personal privacy. To be fully effective, however, a privacy amendment should be adopted only after a detailed public examination of the costs and benefits of a constitutional commitment to personal privacy.[40] Given the political complexities of the amendment process—especially in Minnesota[41]—it appears that the better approach, for the immediate future, would be to provide more protection for data privacy by statute.

III. THE MINNESOTA DATA PRIVACY ACT

A majority of states have enacted statutes governing various aspects of informational privacy.[42] Most take a topical approach, guaranteeing a measure of data privacy within such narrow contexts as taxation, education, welfare, and state employment.[43] A topical approach, however, can offer little general protection for informational privacy concerns. Minnesota was the first of several states to recognize this deficiency and take steps to correct it by enacting comprehensive legislation stressing minimal principles of "fair information practices."[44]

Like other recently enacted comprehensive data privacy statutes,[45] the Minnesota Data Privacy Act,[46] originally adopted by the

40. For example, a preliminary public dialogue on data privacy is being held in Minnesota from April through June 1978, supported by a special grant from the Minnesota Humanities Commission. As part of this program, conferences on the data privacy issue are scheduled for cities throughout the state.

41. *See* Mitau, *Constitutional Reforms in Minnesota—Change by Amendments, 1947-1977*, in PERSPECTIVES ON MINNESOTA GOVERNMENT AND POLITICS 55 (M. Gieske & E. Brandt eds. 1977).

42. For a compilation of state informational privacy statutes, see PRIVACY PROTECTION STUDY COMMISSION, *supra* note 1, app. 1, at 29-85 (Privacy Law in the States).

43. Delaware's law is a good example of the topical approach to informational privacy. The Delaware Freedom of Information Act, DEL. CODE tit. 29, §§ 10001-10005 (Supp. 1977), contains exemptions for personnel, medical, and educational files and for records exempted by statute or common law, including driving records, public assistance records, adoption records, school records, arrest records, and juvenile court records. *See generally* PRIVACY PROTECTION STUDY COMMISSION, *supra* note 1, app. 1, at 38 (Privacy Law in the States).

44. MINN. STAT. § 15.162 (1976).

45. *See, e.g.*, ARK. STAT. ANN. §§ 16-801 to -810 (Supp. 1977); CONN. GEN. STAT. ANN. §§ 4-190 to -197 (West Supp. 1978); MASS. GEN. LAWS ANN. ch. 66A, §§ 1-3, ch. 214, § 3B (West Supp. 1977); OHIO REV. CODE ANN. §§ 1347.01-.99 (Page Supp. 1977); VA. CODE §§ 2.1-377 to -386 (Supp. 1977).

46. MINN. STAT. §§ 15.162-.169 (1976 & Supp. 1977).

Legislature in 1974,[47] parallels the Federal Privacy Act of 1974.[48] The goal of such comprehensive data privacy legislation is threefold: (1) to facilitate the correction of inaccurate records by ensuring data subjects access to information about themselves; (2) to impose duties on governmental agencies to exercise reasonable precautions against misuse of personal data and to generally govern the disclosure of data to third parties; and (3) to provide, with varying degrees of coverage, some legal remedies to individuals to effectuate their informational privacy rights.[49]

The Minnesota Privacy Act regulates the classification and dissemination of any records, files, or processes that identify an individual and that are retained or intended to be retained on a permanent or temporary basis.[50] The Act stipulates that information may be classified as *public*,[51] *private*,[52] or *confidential*,[53] but provides no guidelines concerning how specific types of information should be categorized.

Public data is defined to include all information that is accessible to the general public.[54] Every custodian of public records is required to keep public data in such an arrangement and condition as to make them readily accessible for convenient use.[55] Except as otherwise provided by law, he must permit all public data to be inspected, abstracted, or copied at any reasonable time and, upon demand and payment of fees, furnish certified copies thereof.[56] *Private data* denotes information that is accessible to the subject of the information but not to the public.[57] Private data generally cannot be collected,

47. Act of Apr. 11, 1974, ch. 479, 1974 Minn. Laws 1199 (codified at MINN. STAT. §§ 15.162-.169 (1976 & Supp. 1977)). Since 1974, the Data Privacy Act has been frequently amended. *See* Act of Apr. 5, 1978, ch. 790, 1978 Minn. Sess. Law Serv. 1012 (West); Act of June 2, 1977, ch. 375, 1977 Minn. Laws 825; Act of Apr. 13, 1976, ch. 283, 1976 Minn. Laws 1063; Act of Apr. 9, 1976, ch. 239, §§ 2-6, 1976 Minn. Laws 880; Act of June 5, 1975, ch. 401, 1975 Minn. Laws 1353.

48. 5 U.S.C. § 52a (1976).

49. Virginia is the only state with a comprehensive informational privacy act that does not provide at least some form of legal recourse for aggrieved data subjects. Arkansas, Massachusetts, Minnesota, and Utah permit both compensatory and punitive damages and allow for recovery of attorneys' fees. The Ohio statute does not permit the recovery of attorneys' fees, but makes information obtained in violation of disclosure provisions inadmissible as evidence in a legal proceeding. *See generally* PRIVACY PROTECTION STUDY COMMISSION, *supra* note 1, app. 1, at 5 (Privacy Law in the States).

50. MINN. STAT. §§ 15.162-.167 (1976 & Supp. 1977).

51. MINN. STAT. § 15.162(5b) (1976).

52. *Id.* § 15.162(5a).

53. MINN. STAT. § 15.162(2a) (Supp. 1977).

54. MINN. STAT. § 15.162(5b) (1976).

55. *Id.* §§ 15.162(5b), .17(4).

56. *Id.* § 15.17(4).

57. *Id.* § 15.162(5a).

stored, used, or disseminated for any purpose other than that stated to the data subject at the time of collection.[58] *Confidential data* is defined as any information that is accessible to neither the individual subject nor the public.[59]

The officials responsible for the collection, use, and dissemination of any data on individuals are designated by law or by the Commissioner of Administration as *responsible authorities.*[60] Every responsible authority is charged with limiting the collection, storage, use, and dissemination of data to that necessary for the administration and management of programs specifically authorized by the Legislature or local governing body or mandated by the federal government and with establishing procedural safeguards to ensure that all public, private, or confidential data on individuals are accurate.[61] A responsible authority must periodically submit to the Legislature a description of each category of record, file, or process relating to private or confidential data on individuals maintained by his agency.[62]

The Data Privacy Act confers explicit legal rights on data subjects. An individual asked to supply private or confidential data concerning himself must be informed by the collecting state agency of the purpose and intended use of the requested data, any right he may have to refuse to supply the requested data, any known consequence arising from his supplying or refusing to supply such information, and the identity of other persons or entities authorized by state or federal law to receive the data.[63]

An individual also has the right to be informed whether he is the subject of stored data and whether such data are classified as public, private, or confidential. A subject of stored data must be shown public and private data without expense and be informed of the content

58. *Id.*

59. MINN. STAT. § 15.162(2a) (Supp. 1977). One significant change made by the 1976 Legislature was the creation of an "emergency data classification system" under the authority of the Commissioner of Administration. *See id.* § 15.1642. An agency of state or local government may apply to the Commissioner "on an emergency basis" to have information classified as private or confidential. *Id.* § 15.1642(1). The party seeking the classification must demonstrate that no statute exists that would allow or forbid a classification of the information as private or confidential, that data for which the application is being sought have been treated similarly in the past, and that a compelling need exists for the classification. *Id.* § 15.1642(2). If the Commissioner of Administration concurs in the classification, it is submitted to the Attorney General for approval; if he does not, the data become public data. *Id.* § 15.1642(3). The Legislature is to make final determinations on such classification, apparently by statute. *Id.* § 15.1642(1).

60. *Id.* § 15.162(6).

61. MINN. STAT. § 15.1641 (1976).

62. *Id.* § 15.163.

63. MINN. STAT. § 15.165 (Supp. 1977).

and meaning of those data.[64] A data subject may, upon notification in writing to the appropriate responsible authority,[65] contest the accuracy or completeness of public or private data, and the determination of the responsible authority may be appealed pursuant to the provisions of the Administrative Procedure Act.[66]

A responsible authority who violates any provision of the Minnesota Data Privacy Act is liable to a person who suffered damage as a result of the violation;[67] an injured person may also initiate an action against the relevant political subdivision for damages sustained, plus costs and reasonable attorneys' fees.[68]

IV. TOWARD AN IMPROVED DATA PRIVACY ACT— SOME CRITICISMS AND SUGGESTIONS

The Minnesota Data Privacy Act, while commendable as an initial effort, simply does not go far enough to protect emerging expectations of informational privacy. Perhaps in recognition of this fact, the Minnesota Legislature in 1975 created the Joint Legislative Privacy Study Commission to conduct a detailed public analysis of the data privacy problem.[69] Although the Commission found it necessary to narrow the scope of its study,[70] and was thus unable to furnish the comprehensive report requested by the Legislature,[71] it did present a number of significant recommendations to strengthen the data privacy statute.

64. *Id.*

65. *Id.*

66. MINN. STAT. § 15.1641 (1976).

67. *Id.* § 15.166.

68. *Id.*

69. The Privacy Study Commission was established for the purpose of studying and investigating the collection, storage, use, and dissemination of data on individuals by political subdivisions, state agencies, statewide systems, and any other public or private entity in the state. *See id.* § 15.169. The Commission included Senators Eugene Merriam, John Keefe, and Robert Tennessen, and Representatives John Lindstrom, John Arlandson, Willian Dean, and B.J. Philbrook. The Commission had four major responsibilities: (1) to determine whether executive orders, attorney general opinions, regulations, laws, and judicial decisions in the area of data privacy are consistent with individual privacy and other constitutional guarantees; (2) to determine the effect of federal law on collection, storage, use, or dissemination of personal data; (3) to analyze the standards and criteria governing programs, policies, and practices relating to the use of personal data; and (4) to collect all available information pertaining to the data privacy issue. *See id.*

70. The Data Privacy Commission limited its efforts to making recommendations for improving privacy protection in the areas of public welfare and law enforcement and the practice of purchasing lists of names from state agencies for mass mailings. *See generally* JOINT HOUSE-SENATE PRIVACY STUDY COMMISSION, REPORT TO THE MINNESOTA LEGISLATURE 3 (1976) [hereinafter cited as MINNESOTA PRIVACY REPORT].

71. *Id.*

Unfortunately, legislative response to the findings of the Privacy Commission has been minimal,[72] perhaps because of analytical and political difficulties surrounding informational privacy. To aid policymakers dealing with the complexities of this issue, the Article will expand upon a number of the most significant observations of the Privacy Commission and examine some deficiencies in the Data Privacy Act that were not discussed by the Commission. While this critique cannot provide an exhaustive analysis of the data privacy question, it is hoped that a discussion focused on the most critical aspects of the problem will illuminate future legislative discussion.

A. Minimizing Data Ingestion

Among the Commission's major findings were the observations that too much information is collected by many governmental agencies[73] and that "much of the data collected is unnecessary or irrelevant to agency activities."[74] The Commission found that these problems resulted, in part, from a lack of specific statutory guidelines for data collection.[75]

The collection of information from the data subject is the beginning of the data privacy relationship. Whenever personal information is collected by a governmental agency, there is potentially a loss of privacy to the data subject.[76] Government, however, must remain accountable to the governed, and the flow of information in the public sector is necessary to measure the efficacy of public programs. Thus, to the extent that the data subject provides information in order to receive governmental services or other state-conferred benefits, he may have to bear some risks arising from disclosure of personally sensitive data. If the individual understands the risks and benefits, or if he can command competent legal assistance, he may be able to make an intelligent choice between providing the data and forgoing the benefits.

---

72. The 1977 Legislature enacted various definitional and procedural changes to bring the statute in line with the provisions of federal law. *See* Act of June 2, 1977, ch. 375, 1977 Minn. Laws 825 (codified at Minn. Stat. §§ 15.162, .1642, .165 (Supp. 1977)). The 1978 Session of the Legislature acted to extend to July 31, 1979, the expiration date of the emergency classification system, *see* note 59 *supra*, and to prohibit dissemination of government-held data to Interpol, an international private investigative organization. *See* Act of Apr. 5, 1978, ch. 790, 1978 Minn. Sess. Law Serv. 1012 (West).

73. *See* Minnesota Privacy Report, *supra* note 70, at 6.

74. *Id.*

75. *See id.* The Commission also found that too much information is collected because of administrative willingness to cooperate with federal and state statistical research. *See id.* at 9-10.

76. *See* Whalen v. Roe, 429 U.S. 589, 605 (1977), *quoted at* text accompanying note 29 *supra*.

An individual's competency in privacy matters is, however, seldom adequate. In an experiment conducted in a Georgia mental health assistance program, data collection dropped from 100% to 20% after subjects were informed that failure to provide information would not result in any loss of services.[77] Furthermore, there are some instances in which the individual cannot control the collection of data, such as where information is obtained from third parties.

As a general proposition, therefore, minimizing data ingestion is a vital objective. It is, however, an objective that is difficult to achieve. Although broad agreement could probably be reached with respect to certain types of data collection that should be proscribed altogether, such as where information is sought concerning an individual's political activities or the organizations with which he associates,[78] complete categorization efforts would require consensus on a number of subtle ethical, personal, and social issues. Rather than attempting the endless series of detailed qualifications such an effort would demand, attention should be focused on providing broad legislative standards for minimizing the ingestion of data.

The Minnesota Legislature might begin by enacting a statutory policy statement clearly setting forth a commitment to "minimum intrusiveness," a goal of the Federal Privacy Act[79] and an objective of the Federal Privacy Protection Study Commission.[80] Assuming an established need for information, minimum intrusiveness means that a specified piece of information should only be gathered if it is not extraneous to that need. As the Minnesota Privacy Study Commission observed, such a goal has not always been achieved by state agencies.[81] For instance, the Commission found that a job application form used by the Minnesota Department of Public Welfare for a position that required a valid driver's license asked whether the applicant's license had ever been suspended or revoked.[82] The Commission suggested that it is not necessary to know such information to determine that an applicant is a qualified driver. Thus, the Commission recommended that all forms requesting data should be specifically and narrowly drawn so that they do not ask for unnecessary or irrelevant information.[83]

77. *See* A. WESTIN, COMPUTERS, HEALTH RECORDS, AND CITIZEN RIGHTS 243-44 (NBS Monograph No. 157, 1976).

78. *See, e.g.,* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958).

79. 5 U.S.C. § 552a (1976).

80. PRIVACY PROTECTION STUDY COMMISSION, *supra* note 1, at 14-17. The object of minimum intrusiveness is "to create a proper balance between what an individual is expected to divulge to a record-keeping organization and what he seeks in return." *Id.* at 14.

81. *See* MINNESOTA PRIVACY REPORT, *supra* note 70, at 6.

82. *See id.* at 10.

83. *See id.*

While the existing Data Privacy Act purports to limit the collection of data to those "necessary for the administration and management of programs specifically authorized,"[84] the state's commitment to minimizing data ingestion has been hampered by the lack of uniform standards of necessity.[85] This problem could best be addressed by a statute directing the Department of Administration to conduct a continuing evaluation of the information collected by state agencies, which in turn could form the basis of comprehensive regulations governing data ingestion.

It must also be recognized that any collection of data from an individual involves a certain cost to society in that personal privacy is thereby diminished. This cost should be explicitly acknowledged by the Legislature: any policy action that requires the collection of new data from individuals should be accompanied by some measurement of the extent to which the action imposes on privacy.

All of these objectives—ensuring minimal intrusiveness, evaluating necessity, and analyzing societal costs and benefits—could be facilitated by requiring a "privacy impact statement" for all new legislative and administrative programs. While not approaching the technical complexity of an environmental impact statement,[86] a privacy impact statement could provide an index of privacy costs before a program was actually adopted by requiring the proponents of a particular program to evaluate it in light of a number of considerations:

> (1) *Quantitative Intrusiveness*—a calculation of the number of data required by the program and the cost of collecting and maintaining those data;
>
> (2) *Qualitative Intrusiveness*—an assessment of the impact of the data collection requirements on those residual areas of privacy recognized as critical by the courts[87] and the public;
>
> (3) *Collection Technique*—a description of the method of data collection,[88] with special emphasis on the distinction between primary and secondary collection;[89]

---

84. MINN. STAT. § 15.1641(b) (1976).

85. *See* text accompanying notes 73-75 *supra.*

86. *See* MINN. STAT. § 116D.04 (1976).

87. *See, e.g.,* Doe v. Bolton, 410 U.S. 179 (1973) (personal health); Griswold v. Connecticut, 381 U.S. 479 (1965) (family matters); Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539 (1963) (membership and contribution records); Ravin v. State, 537 P.2d 494 (Alas. 1975) (personal activity within one's home).

88. If the collection procedure necessitates the subject's informed consent, *see* text following note 76 *supra,* the statement should also specify the procedure for obtaining consent.

89. "Primary data collection" is the process of collecting data directly from the

(4) *Expected Use and Dissemination*—an identification of the intended use of data by administrative agencies;[90]

(5) *Anticipated Length of Retention*—an estimate of the time period during which the data will continue to be accurate and useful for their stated purpose;[91]

(6) *Responsible Authority*—a designation of the officials responsible for data collection, use, and dissemination.[92]

Operationally, the privacy impact statement could be built upon the experience of the Office of Management and Budget in implementing the Federal Privacy Act of 1974.[93] To comply with the requirement that Congress be given notice of any proposal to establish or alter a system of personal data,[94] the Office of Management and Budget established a set of threshold conditions for determining when such a notice must be filed.[95] In a Minnesota adaptation, a privacy impact statement could be required whenever (1) legislative funding or authorization is sought for a new program that requires collection of personal information; (2) a change is proposed in an existing system of records that would increase the number of individual data subjects, expand the types of data collected, or increase the quantity of data collected; (3) a change in the storage system for personal information is proposed; (4) an alteration in the purpose for which data are to be collected or used is suggested; or (5) new regulations are proposed to change procedures for data collection, storage, use, or dissemination.

---

data subject; "secondary data collection" is the process of collecting data from third parties.

90. Agency officials should identify (1) the intended procedures for data storage, (2) the agencies or individuals that will be given access to the data, and (3) the contemplated method of notifying data subjects of any changes in the use of personal data pertaining to them.

91. When the data are no longer useful for their stated purpose, explicit justification should be required for permanent storage, without which the data would have to be removed from the system. *See* notes 110-13 *infra* and accompanying text.

92. A system-wide index, naming the responsible authorities for data and classifying the data by type or program subject should be maintained as a public document, formally filed and kept current. Such a designation system would provide aggrieved individuals or their advocates a means of establishing agency and individual responsibility for data misuse.

93. 5 U.S.C. § 552a (1976).

94. Each agency shall provide adequate advance notice to Congress and the Office of Management and Budget of any proposal to establish or alter any system of records in order to permit an evaluation of the probable or potential effect of such proposal on the privacy or other personal or property rights of individuals or the disclosure of information relating to such individuals, and its effect on the preservation of the constitutional principles of federalism and separation of powers.

Id. § 552a(o).

95. *See* 40 Fed. Reg. 45,877 (1975).

If the impact statement accompanies new legislation, it should be appended to the authorizing bill and become subject to the same hearing process.[96] If it is supplied in relation to changes in existing information systems, it should be reviewed by either a standing committee of the Minnesota Legislature or the Legislative Audit Commission.[97] In addition to estimating privacy costs in policy development, the impact statement could serve as part of a legislative authorization mechanism for the collection of data, replacing the currently ineffective general authorizations granted as a part of agency power.[98]

While the privacy impact statement would offer a process to strengthen legislative oversight of the collection of data in general, it would not in itself serve as a statutory safeguard against excessively intrusive data collection. Standards that will provide the courts with meaningful guidance in balancing privacy claims against the state's interests in public health, welfare, safety, and order must be written directly into legislation. Thereafter, administrators could formulate information collection policy with the knowledge that an overbroad collection would constitute a violation of the statute.

For data collection concerning such sensitive areas as religion, association, health, or family matters, the Legislature should require the agency to demonstrate that the information is necessary to a compelling state interest. For less sensitive areas, a less rigid standard of reasonable necessity would be sufficient so long as the need for such information is justified in terms of the purpose for which the agency was created. Mere incantations of public necessity, safety, order, welfare, convenience, or administrative symmetry, however, should not be persuasive. If the normative legislative policy standards are to be meaningful, they must shift the burden of demonstrating the need for data collection to the governmental agency, which must then articulate completely the policy basis on which it seeks information.

B. Safeguarding Data Storage and Use

The Minnesota Privacy Commission found several problems with the provisions of the Data Privacy Act dealing with data storage

96. *See generally* J. Davies, Legislative Law and Process in a Nutshell 89, 162-63 (1975).

97. *See* Minn. Stat. § 3.97 (1976).

98. The Minnesota Privacy Study Commission cited Minn. Stat. § 257.33 (1976) as an example of vague and open-ended legislation. *See* Minnesota Privacy Report, *supra* note 70, at 21-22. Because section 257.33 so broadly defines the duties of the Commissioner of Public Welfare, personal data regarding matters such as illegitimate births are collected without restriction and without regard for the Welfare Department's need for the information.

and use.[99] The Commission recommended that the statute's classification system be revised to establish a procedure for determining how long public records should be stored.[100]

Any attempt to regulate data management requires an understanding of its relationship to other aspects of informational privacy.[101] Once information has been collected, any use thereof or any decision with respect to it may compromise personal privacy. Classification of data may have implications for personal rights of access, while dissemination of data may affect the individual's ability to control who sees the data. Likewise, storage of data over a long period of time may affect privacy because of the insecurity of data storage and the tendency of data to become inaccurate.

The nature of the data management problem demands a general legislative policy statement to guide particular agency decisions. In the absence of formally articulated constraints in the current Data Privacy Act, executives and administrators are left with wide discretion in the implementation of the law. The mechanism that supposedly governs the use and disclosure of personal data—the data classification system—provides only that data are to be classified as public, private, or confidential.[102] It neither defines these terms by types of data nor provides general criteria for data classification.

The problem of overbroad agency discretion is exacerbated by certain facts of administrative life. The need to reduce the unanticipated consequences of administrative decisions gives rise to organizational imperatives toward maximizing the data base for decisionmaking.[103] If a program operates in human service fields, this extensive

---

99. *See* MINNESOTA PRIVACY REPORT, *supra* note 70, at 10-13 (discussing MINN. STAT. § 15.17 (1976)).

100. *See id.*

101. An agency's data management responsibilities encompass all aspects of the privacy relationship—collection, storage, use, and dissemination.

> [T]he fact that an organization may use its records about individuals in accounting for its operations to other centers of power and authority in society. . . has important implications for any policy of record-keeping regulation. It prompts caution in considering prohibitions on the collection of items of information from or about individuals, but at the same time draws attention to the need for special safeguards when requiring an organization to record any information about an individual that it does not need to facilitate its own relationship with him.

PRIVACY PROTECTION STUDY COMMISSION, *supra* note 1, at 9.

102. *See* text accompanying notes 51-59 *supra.*

103. *See generally* Shackle, *Decision: The Human Predicament,* ANNALS, March 1974, at 1. According to Shackle, the motivation is to reduce unanticipated second and third order consequences that may arise if decisions are made on the basis of inadequate information by "perfecting" (increasing the size of) the data base. *See id.* Sociologist Daniel Bell goes one step further, treating information as a resource that can form the basis of political and social power. *See generally* D. BELL, THE COMING OF POST-INDUSTRIAL SOCIETY (1973).

data collection often unavoidably intrudes into personally sensitive areas.[104] Moreover, agencies designed to perform such functions as building highways or enforcing the law frequently view data security and informational privacy rights as unwarranted and burdensome demands.[105] Conscious of public pressures for accountability and high expectations of performance, they perhaps understandably view privacy concerns as secondary to their program tasks. Thus, the absence of legislatively imposed constraints results in insufficient organizational attention to legitimate individual expectations of informational privacy.[106]

A primary goal of the next legislative session should be an improved data classification system. This revision should delineate the types of data to be placed in each category. The *confidential* classification[107] presents a particular problem, since that label currently limits the individual's right to see and perhaps correct data about himself. Some safeguards are clearly necessary to avoid inconsistencies and abuses in the application of the classification. An individual who is the subject of confidential data should, at a minimum, be given notice of that fact.[108] The data subject should also have an opportunity for a hearing to challenge the classification.

A second goal of data management policy in Minnesota should be to ensure that all stored data are accurate and timely, in addition to being necessary for the administration of a state agency or program. Even with the data ingestion controls suggested previously, a considerable number of data about individuals will continue to be gathered. As the Federal Privacy Protection Study Commission noted, however, accurate data do far less harm than data that are false, deleterious, or otherwise potentially dangerous.[109]

---

104. *See generally* PRIVACY PROTECTION STUDY COMMISSION, *supra* note 1, at 458-59.

105. *See generally* Baker, *Record Privacy as a Marginal Problem: The Limits of Consciousness and Concern*, in SURVEILLANCE, DATAVEILLANCE AND PERSONAL FREEDOMS, *supra* note 2, at 100-02.

106. *See generally id.* Baker's analysis of recordkeeping proceeds on two levels. First, recordkeeping is largely a marginal activity, a nuisance for an organization that operates on a set of goals, such as welfare payment, education, or preservation of order, rather than an orientation to single individuals. Second, recordkeeping processes are largely invisible to the subjects of data; consequently, it is unlikely that individuals will come forward and pressure the recordkeeper into a concern for civil rights and civil liberties.

107. MINN. STAT. § 15.162(2a) (Supp. 1977).

108. In cases where the data subject's psychological or medical condition may be adversely affected by knowledge of the confidential data, it may be appropriate to appoint a guardian who can discuss classification problems on behalf of the data subject.

109. *See generally* PRIVACY PROTECTION STUDY COMMISSION, *supra* note 1, at 17-19.

To avoid the danger to privacy inherent in the very existence of data inaccuracies, a relatively simple principle should become the rule of data management in Minnesota: where information is unneeded, it should be thrown away. To effectuate this goal, zero-based information management systems[110] could be integrated into existing program audit and evaluation systems for state and local service programs.[111] This process would entail a periodic examination of the agency's stored information resources in light of present agency responsibilities and would require a demonstration that the system does not retain unnecessary, false, or inaccurate data. Each agency holding personal data that it wished to retain would be required to conduct an annual audit of such data under the direction of the Department of Administration. Such an audit should address several questions:

(1) Do the data duplicate other information held by the same agency?

(2) Are data about an individual stored at more than one location within the same agency?

(3) Are the data current?

(4) Are the data accurate?

(5) Does the individual file contain hearsay, third party recollections, or impressions?

(6) Has any attempt been made to verify the data?

---

110. Zero-based information management is analogous to zero-based budgeting, which was developed by Texas Instruments, Inc., in 1969 and applied to the Georgia state budget in 1973 by then-Governor Jimmy Carter. *See generally* Pyhrr, *The Zero-Base Approach to Government Budgeting*, 37 PUB. AD. REV. 1 (1977)..

A precedent for zero-based information management has been provided by courts and legislatures that have recognized the dangers in retaining certain criminal records and have attempted to regulate the retention of such data. *See, e.g., In re* R.L.F., 256 N.W.2d 803 (Minn. 1977), *noted in* Comment, *Criminal Procedure: Expungement of Arrest Records*, 62 MINN. L. REV. 229 (1978); MINN. STAT. § 152.18 (1976). Twenty states have legislation that provides for at least some form of expungement of non-conviction information; seven states expunge conviction information following a period of good behavior. There are also a number of cases supporting, on constitutional grounds, the return of unneeded and potentially damaging data. Eddy v. Moore, 5 Wash. App. 334, 487 P.2d 211 (1971), was the first case to recognize explicitly the link between the return or removal of potentially damaging information and the right of privacy: "There is a direct correlation between the loss of individual privacy and the retention of arrest records." *Id.* at 342, 487 P.2d at 216. *See generally* United States v. Kalish, 271 F. Supp. 968 (D.P.R. 1967) (ordering information expunged from Justice Department files); *see also* Menard v. Saxbe, 498 F.2d 1017 (D.C. Cir. 1974) (ordering the removal of fingerprints from the FBI's centralized files on statutory grounds).

111. Generally, the State Auditor is responsible for existing audit and evaluation systems. *See* MINN. STAT. §§ 6.01-.71 (1976). Specifically, a zero-based management system could be added to section 6.65.

The burden should be on the agency to respond to these concerns. If this cannot be done and the individual's relationship to the agency is such that an extensive information profile need not be retained, the data should be removed from the information system.

Individual citizens should also be involved in the zero-based data management system. Data subjects whose files contain sensitive personal information should be notified of the existence of their files when the datakeeping agency conducts its audit. Such notice would allow the data subject the opportunity to contribute his knowledge of the file's accuracy to the audit process. The individual should not, however, be forced to wait for the audit process to challenge the accuracy of a file. The provisions of the present law should be expanded to place an ongoing duty on the dataholding agency either to make requested corrections and deletions or to audit the file immediately for accuracy and currency.

Zero-based data management and storage systems will further data privacy concerns not only during the period of data retention, but also at the time of collection,[112] by increasing accuracy and by raising administrative sensitivity to data privacy issues. The intent of the system is not to place impossible demands on public administrators but to alter institutional priorities, which currently place little emphasis on the personal expectations of informational privacy.[113] In addition, it is hoped that this system would remove at least a large portion of the unnecessary and potentially dangerous information currently in state storage systems without placing burdens on the individual to initiate removal through legal or administrative processes.

C. Strengthening Individual Rights and Remedies

No set of legislative policies or administrative regulations can provide absolute assurance that individual expectations of informational privacy will always be fulfilled. Although the dangers to the individual data subject may be reduced through proper collection and dissemination controls, they cannot be fully eliminated. The existing Minnesota Data Privacy Act attempts to remedy this problem by granting data subjects the right to review their files and suggest corrections,[114] except where the files are classified confidential.[115]

112. The task of justifying stored data would presumably encourage administrators to collect only those data that are necessary, reinforcing the suggested ingestion controls.

113. *See* text accompanying notes 103-06 *supra.*

114. *See* Minn. Stat. § 15.165(c) (1976).

115. *See id.* § 15.165(b).

Data subjects also have the right to sue for damages resulting from violations of the Act.[116]

The enforcement of these remedies, however, requires the individual citizen to possess an extraordinarily high order of analytical and legal competence. The data subject must identify data locations, be aware of procedures for access, and understand his legal rights.[117] In addition, the citizen must deal with administrative agencies that do not always give high priority to informational privacy concerns.[118]

Minnesota's Data Privacy Act does little to ease this burden of competence on the data subject. For example, mere knowledge of the existence of a confidential file may be an inadequate basis for bringing a remedial action because in many cases only an examination of the file itself can show whether a cause of action exists. Thus, closure of confidential files may seriously curtail effective and realistic redress. Moreover, to secure an administrative remedy under the Data Privacy Act, the data subject must bring his dispute under the provisions of the Minnesota Administrative Procedure Act,[119] which provides that in contested cases all interested parties shall receive a hearing before a hearing examiner.[120] Under the Procedure Act, however, "filings, testimony, and exhibits" presented in a contested data privacy case would constitute part of the hearing examiner's "official record"[121]—a *public* record.[122] Thus, the administrative remedy for some informational privacy violations appears to require the data subject to open his confidential files to the public.

Considerations of privacy aside, the hearing process itself usually requires legal counsel.[123] Appeals to the courts may impose additional litigation costs before a final resolution is achieved. Thus, under present Minnesota law, an individual must assume the burden of securing his own privacy expectations, which presumes legal competence and resources that most people do not have. Opportunities for nonjudicial

116. *See id.* § 15.166(1).

117. *See* Baker, *supra* note 105, at 102-03. Even where the data subject has knowledge of recordkeeping practices, protection of personal privacy requires the individual to expend time, money, and energy.

118. *See generally id.* at 100-02.

119. MINN. STAT. §§ 15.0411-.0426 (1976).

120. *See id.* § 15.0418.

121. *See id.*

122. "All officers . . . of the state . . . shall make and keep all records necessary to a full and accurate knowledge of their official activities. All such *public* records shall be . . . of such quality as to insure permanent records." *Id.* § 15.17(1) (emphasis added). Furthermore, under the terms of the Minnesota Open Meeting Law, the hearing cannot be closed. *See id.* § 471.705(1).

123. Hearings employ technical evidentiary rules and cross-examination procedures that presume a relatively high level of legal competence. *See generally id.* § 15.0419.

resolution of matters of this kind, though recommended by many within the legal profession,[124] are limited under existing Minnesota law. It seems appropriate that such opportunities be expanded by a revised fair information practices policy.

Sweden's Data Act of 1973[125] suggests that the burden of remedial action rests on the state, as the keeper of data.[126] Although Sweden's law imposes specific obligations on the datakeeper for accuracy and verification of data,[127] the concept need not be limited to these tasks. As a general proposition, the State of Minnesota, as the keeper of data on its citizens, should assume the burden of providing reasonable remedial processes that would not involve burdens of extensive litigation.

Remedies to enforce informational privacy must serve two functions if they are to be considered successful. First, some mechanism must be found to assist citizens in identifying and examining their informational privacy problems. This "ombudsman" function serves to provide data privacy expertise to citizens seeking assistance. Second, a nonjudicial resolution of privacy disputes must be established to reduce litigational costs for the average citizen and to prevent most such disputes from reaching crowded court dockets. This "mediation" function should also be a part of a comprehensive policy regarding individual privacy rights and remedies.

California has chosen to combine both functions in an Office of Information Practices.[128] Specifically, the responsibilities of the Office include assisting individuals in the identification of records that may contain personal information, investigating violations of the Information Practices Act, determining whether a violation has occurred, reporting violations to the Governor and Attorney General,

124. Nonjudicial remedies for resolution and prevention of disputes between individuals and governmental agencies have been suggested by the second American Assembly on Law and a Changing Society. The Assembly has endorsed the use of publicly funded ombudsmen and information mediation techniques. *See Final Report of the American Assembly on Law and a Changing Society II,* 61 A.B.A.J. 931, 934 (1975).

125. Law of May 11, 1973, [1973] Svensk Författningsamling [SFS] 289 (Swed.), *reprinted in* DATA PROTECTION LEGISLATION 129-40 (U. Damman, O. Mallmann, & S. Simitis eds. 1977).

126. *See generally id.* §§ 8-24.

127. The duties imposed on the "responsible keeper of the register" are (1) to make necessary verifications and correction in data held; (2) to ascertain the completeness of the information; (3) to inform the data subject of information held on him; (4) not to release information that may be used contrary to the Act; (5) not to make data on individuals public without authorization. *See id.* §§ 8-14. The significant contribution of the Swedish model is the obligation it places on the datakeeper to protect informational privacy rights.

128. *See* CAL. CIV. CODE §§ 1798.4-.8 (West Supp. 1978).

and developing model guidelines for the implementation of the Information Practices Act.[129] The Office also provides mediation service for individuals and agencies that do not choose to resort to court action.[130]

In Minnesota these functions could be served separately by creating a "Privacy Ombudsman" and expanding the authority of the Legislative Audit Commission. Ombudsman models of citizen advocacy,[131] currently used in several states,[132] could be adapted to data privacy disputes with little difficulty. An ombudsman's duties could include direct investigation of individual privacy complaints, investigation of data security arrangements, and commencement of court actions to enjoin unnecessary or deleterious collection of data by other state agencies.[133] The Minnesota Legislative Audit Commission

129. *See id.* §§ 1798.4-.7.

130. *See id.* § 1798.8. Although mediation is available, aggrieved data subjects are not required to resort to mediation before pursuing other remedies. *See id.*

131. "Ombudsman" is used to denote an office established by the legislature and headed by an independent public official. The ombudsman, after receiving a complaint against a governmental agency, official, or employee, would conduct an investigation and on the basis of his findings recommend corrective action in those cases where the complaint was justified. *See* Frank, *State Ombudsman Legislation in the United States*, 29 U. MIAMI L. REV. 397, 397-98 (1975).

132. *See, e.g.*, ALASKA STAT. §§ 24.55.010-.340 (1976); HAW. REV. STAT. §§ 96-1 to -19 (1976); IOWA CODE §§ 601G.1-.23 (1977). For a comparative analysis of state ombudsman statutes, see Frank, *supra* note 131.

133. A framework for ombudsman legislation has been suggested by the American Bar Association's Ombudsman Committee. *See* ABA MODEL OMBUDSMAN STATUTE FOR STATE GOVERNMENTS (1974), *reprinted in* Frank, *supra*.note 131, at 402-43. Minnesota may wish to adopt section 11 of the ABA Model Act:

> The Ombudsman shall have the following powers:
> (a) to investigate, on complaint or on his own motion, any act of an agency without regard to its finality;
> (b) to adopt, promulgate, amend and rescind rules and regulations required for the discharge of his duties—including procedures for receiving and processing complaints, conducting investigations, and reporting his findings—not inconsistent with this Act. However, he may not levy any fees for the submission or investigation of complaints;
> (c) to examine the records and documents of any agency;
> (d) to enter and inspect without notice the premises of any agency;
> (e) to subpoena any person to appear, to give sworn testimony or to produce documentary or other evidence that is reasonably material to this inquiry;
> (f) to undertake, participate in or cooperate with persons and agencies in such conferences, inquiries, meetings, or studies as might lead to improvements in the functioning of agencies;
> (g) to obtain such information and make such inquiries from any agency or person as he shall require for the discharge of his duties;
> (h) to maintain secrecy in respect to all matters and the identities of the complainants or witnesses coming before him;
> (i) to bring suit in [district court] to enforce the provisions of this Act;
> (j) to establish and administer a budget for his office;

could be given mediation jurisdiction over disputes between data subjects and state agencies arising from the operation of the Data Privacy Act or any future informational privacy statute.[134] To avoid privacy problems caused by the currently available review procedure under the Administrative Procedure Act,[135] provision should be made for an *in camera* examination of stored data by the Audit Commission, the individual citizen, and the responsible authority in the dispute.

Since there is little experience with the above described models, it is not yet possible to draw conclusions as to their efficacy in ensuring attention to individual privacy expectations. At this point, however, the emphasis should not be on structural details but rather on ensuring that the services necessary for securing individual rights and remedies are reasonably well provided.

D. A Suggested Fair Information Practices Policy

As the Minnesota Legislature proceeds to refine its approaches to information practices policy and to develop new laws governing the problems of data ingestion, data management, and the rights of individual data subjects, it seems appropriate to consider the normative foundations upon which such a policy could be based. As a key to reform, this "frame of reference" should reflect the major values upon which legislation and administrative regulations could be based. In legislation, it would take the form of a set of legislative findings or a statement of purpose[136] and become the basis upon which implemen-

---

(k) to concern himself with strengthening procedures and practices which lessen the risk that objectionable administrative acts will occur.

Id. § 11, *reprinted in* Frank, *supra* note 131, at 420-21.

134. One approach would be to add the following language to Minn. Stat. § 3.971 (1976):

Powers and Duties of Legislative Auditor . . .

Subd. 3. To resolve disputes arising out of the collection, use, and dissemination of any data on individuals, as defined by Minnesota Statutes, section 15.162(3), the office of the legislative auditor shall be charged with the authority to review and decide appeals pursuant to requested relief from any violation of sections 15.162 to 15.169, committed by the responsible authority stipulated therein.

135. *See* text accompanying notes 119-22 *supra.*

136. The California Information Practices Act of 1977, for example, begins with the declaration that "the right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that *all individuals have a right of privacy in information pertaining to them.*" Cal. Civ. Code § 1798.1 (West Supp. 1978) (emphasis added).

Similarly, the Federal Privacy Protection Study Commission presented three objectives for legislation:

—to create a proper balance between what an individual is expected to divulge to a record-keeping organization and what he seeks in return (*to minimize intrusiveness*);

tational strategies should rest.

First, a legislative policy statement should constitute a recognition that informational privacy is essential to the freedoms of individual citizens. In the absence of effective constitutional protection for informational privacy,[137] this type of commitment would provide administrative and judicial agencies a basis upon which to rest their determinations.

Second, a legislative policy statement should insist that the state, as the keeper of personal data, bear the burden of fairness in the operation of governmental information systems. This burden demands that all actions by an administrative agency with respect to personal information be conducted in such a manner as to promote the rights of individual citizens to informational privacy.

Third, the state's responsibility for fairness should be enhanced by the imposition of a duty on state government to take effective measures to secure the expectations of privacy held by individual citizens. Thus, the state would be committed to providing reasonable means of enabling each citizen to be secure in his expectations of informational privacy.

Although personal expectations of informational privacy certainly represent an important set of values, they are not the only norms that must govern the development of information systems. Privacy must coexist with considerations of openness in government.

Any move toward a more comprehensive data privacy law in Minnesota will face severe scrutiny[138]—and properly so—in view of this state's commitment to openness in government. The legislative manifestation of this ethos of open government, the Minnesota Open Meeting Law,[139] is one of the strictest in the nation.[140] The statute

---

—to open up record-keeping operations in ways that will minimize the extent to which recorded information about an individual is itself a source of unfairness in any decision about him made on the basis of it (*to maximize fairness*); and

—to create and define obligations with respect to the uses and disclosures that will be made of recorded information about an individual (*to create legitimate enforceable expectations of confidentiality*).

PRIVACY PROTECTION STUDY COMMISSION, *supra* note 1, at 14-15.

137. *See* text accompanying notes 15-41 *supra*.

138. The Minnesota Joint Media Committee is one example of a private group active in monitoring changes in privacy legislation. In addition, metropolitan area news organizations have given extensive coverage to privacy considerations. *See* Dawson, *Privacy Battle Lines are Drawn*, St. Paul Pioneer Press, Nov. 14, 1976, § 3, at 1, col. 3; Morrow, *Laws Which Shield Government From Public Eye*, Minneapolis Star, Aug. 1, 1977, § A, at 10, col. 3; Wehrwein, *Limitations on Privacy*, Minneapolis Star, Dec. 22, 1976, § A, at 11, col. 1.

139. MINN. STAT § 471.705 (1976).

140. For a compilation of the various state laws on open meetings, see Guy & McDonald, *Government in the Sunshine: The Status of Open Meetings and Open*

provides that all meetings of any state agency, school district, or other public body be open, except as provided by law.[141] Penalties under the statute are strong; personal civil liability is imposed for violation of the statute, and a third violation can mean loss of office.[142] Judicial interpretations of the law have generally fallen on the side of openness.[143]

Public opinion and the press in Minnesota will continue to insist that the actions and decisions of government be carried out in public view and will invoke the spirit of the first amendment and the Open Meeting Law to enforce their demands. Clearly, some conflict may arise between the competing values of openness and informational privacy.[144] This conflict is probably unavoidable; no macrocosmic solutions have yet been proposed that can accommodate both interests. Yet a strong and carefully drawn fair information practices policy need not foreclose aspirations of public openness. Indeed, such a policy may actually serve to strengthen legitimate insistence on "public business in public." First, it will minimize the ingestion of unnecessary data by state government—data that are potentially dangerous to personal privacy and do not contribute to open government.[145] Second, insistence upon greater accuracy in stored data can

---

Records Laws in North Dakota, 53 N.D.L. REV. 51, 54 n.27 (1976). *See also* UNIVERSITY OF MISSOURI, SCHOOL OF JOURNALISM, FREEDOM OF INFORMATION CENTER REP. No. 354, THE CASE OF OPEN MEETINGS LAWS (1976).

141. *See* MINN. STAT. § 471.705(1) (1976).

142. *See id.* § 471.705(2).

143. *See* Head v. Special School Dist. No. 1, 296 Minn. 267, 208 N.W.2d 294 (1973); Quast v. Knutson, 276 Minn. 340, 150 N.W.2d 199 (1967); Lindahl v. Independent School Dist. No. 306, 270 Minn. 164, 133 N.W.2d 23 (1965); *In re* Minneapolis Area Dev. Corp., 269 Minn. 157, 131 N.W.2d 29 (1964). *See also* OP. MINN. ATT'Y GEN. 10-b (July 3, 1975); *id.* 63a-5 (Feb. 5, 1975); *id.* 471e (Oct. 28, 1974); *id.* 63a-5 (Oct. 28, 1974); *id.* 63a-5 (Dec. 4, 1972); *id.* 63a-5 (Jan. 11, 1972); *id.* 125-a-14 (Sept. 8, 1970); *id.* 471-e (Nov. 2, 1965); *id.* 471e (Sept. 18, 1962); *id.* 471e (Aug. 20, 1962); *id.* 161-A-16(b) (Nov. 20, 1957); *id.* 63-H-5 (June 13, 1957).

144. Financial reporting requirements challenged on privacy grounds have been upheld on the ground that some public interests are so compelling that they may override individual privacy interests. *See* Illinois State Employees Ass'n v. Walker, 57 Ill. 2d 512, 315 N.E.2d 9 (1974). Even in the politically sensitive area of campaign financing, the public's right to know has been held to override expectations that the secrecy of the ballot would extend to campaign contributions. *See* Buckley v. Valeo, 424 U.S. 1 (1976). Thus, it would appear that the courts will continue to balance the competing interests of public accountability and personal privacy on a case-by-case basis.

145. Here a problem of overly simplistic expectations may arise. Michael Baker puts it well:

> [The] generalized allegiance to privacy, confidentiality and due process protections dissolves into a complicated set of opinions as the focus of questioning becomes more specific and the balance between individual liberties and the practical needs of organizations is introduced as an issue. Striking

help to ensure that when data are disclosed their harm to personal privacy interests is minimized. Third, by setting out limited areas where privacy interests should prevail, a legislative fair information practices policy can foreclose attempts to shield what are properly public data behind a ruse of privacy.

Conflict and debate that will arise between these values should be welcomed, not feared. Through the state's political and legal balancing mechanisms—public meetings, the media, the legislature, and the courts—an accommodation of interests may be achieved by experiment and experience.

V. SOME CONCLUDING OBSERVATIONS

This Article has proposed a number of data privacy standards and strategies for governmental information systems. Although the degree to which these standards and strategies may apply to the data privacy issue in the private sector is beyond the scope of this Article, it is increasingly clear that there is a growing public concern for perceived personal privacy violations by banks, credit investigators, employers, and the insurance industry, among others.[146] The interrelationship between governmental and nongovernmental institutions is frequently so close and intimate[147] that norms and practices in one section may have direct implications for the other. After all, large scale corporate organizations exhibit behavioral characteristics quite similar in nature to those of government. A multifaceted and experimental approach toward an effective and comprehensive fair information standards law by the Minnesota Legislature might well contribute not only to the enhancement of credibility in government, but also to the development of policies and practices by nongovernmental institutions for the protection of individual privacy interests.

The purpose of this Article has been to guide the Minnesota Legislature in addressing data privacy issues. Although the existing Data Privacy Act contains several elements that work to protect ex-

---

> a balance between such interests *is* complicated, to be sure, but most individuals do not appear to have the kind of strong consciousness of their own civil liberties interests which might serve as a resource for beginning to deal with record privacy problems.

Baker, *supra* note 105, at 107 (emphasis in original).

146. *See generally* PRIVACY PROTECTION STUDY COMMISSION, *supra* note 1, at 3-6.

147. The Privacy Commission noted that although governmental agencies could use compulsory legal procedures to obtain information from companies issuing credit cards, most of the information conveyed to agencies such as the Internal Revenue Service and the Federal Bureau of Investigation was in response to informal requests by letter, telephone, or personal visit by an agent. *See id.* at 53-55. For example, the Commission estimated that up to 99.5% of the information received by the FBI on credit card holders came through such informal requests. *See id.* at 54.

pectations of personal data privacy,[148] it must be expanded to include an integrated *legislative policy* that would minimize the fragmentation of administrative responsibility for data privacy problems. In general, the Legislature must develop a realistic appreciation of the problems citizens face when they seek to protect their expectations of privacy—expectations that are essential to the establishment of social relationships and the maintenance of personal freedom.

148. *See generally* notes 63-68 *supra* and accompanying text.