Tulsa Law Review

Volume 11 | Number 1

1975

Let Industry Beware: A Survey of Privacy Legislation and Its Potential Impact on Business

Charles W. Pauly

NOTES AND COMMENTS

LET INDUSTRY BEWARE: A SURVEY OF PRIVACY LEGISLATION AND ITS POTENTIAL IMPACT ON BUSINESS

One of the most dramatic outgrowths of the post-Watergate era is the public demand for protection of individual privacy. A concept which is largely undeveloped from a legal standpoint,[1] privacy has suddenly been thrust into the public eye, and is receiving much attention not only by the general public but also in the various legislative branches of government. The current rush towards legislation may result in the imposition of unreasonable burdens upon industry unless the privacy legislation to be enacted is logical, well-reasoned, and limited.

I. PHILOSOPHY

The issue of individual privacy is no more a modern phenomenon than is recordkeeping; both are as old as society itself. They have, however, become of far greater concern to individuals and government as the advances in computer technology have made recordkeeping more practical in terms of its economics and effectiveness and thus more widely employed, and governmental agencies as well as public and private industries have become increasingly dependent upon records about individuals for success in their operation. These two factors are coupled with the rise in public demand for more accountability on the part of government and industry.[2] Within the past few years this concern over privacy has gained acceptance as a vital issue. Recently, the Supreme Court of California remarked:

1. Only three states have statutorily established a cause of action for invasion of privacy, and thirty-four recognize it as an actionable wrong.

2. Address by Dr. Ruth M. Davis, Director of the National Bureau of Standards Institute of Computer Sciences and Technology, National Bureau of Standards of the United States Department of Commerce sponsored conference on, *Government Looks at: Privacy and Security in Computer Systems*, Nov. 19, 20, 1973.

> Cases are legion that condemn violent searches and invasions of an individual's right to the privacy of his dwelling. The imposition upon privacy, although perhaps not so dramatic, may be equally devastating when other methods are employed. Development of photocopying machines, electronic computers and other sophisticated instruments have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds. Consequently judicial interpretations of the reach of the constitutional protection of individual privacy must keep pace with the perils created by these new devices.[3]

Burrows v. Superior Court involved a bank's voluntary compliance with a police investigation by turning over copies of the defendant's bank records. In holding the evidence obtained in this manner to be inadmissible, the court stated:

> [I]n determining whether an illegal search has occurred . . . the appropriate test is whether a person has exhibited a reasonable expectation of privacy and, if so, whether that expectation has been violated by unreasonable governmental intrusion. . . .
>
> . . . .
>
> . . . A bank customer's reasonable expectation is that, absent compulsion by legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes.[4]

Occurrences like those involved in *Burrows* have created a mood in the legislatures and general populace favoring privacy legislation akin to the enthusiasm surrounding the environmental protection movement of a few years ago.

> The private [business] sector should recognize that public interest in an individual's right to privacy is not likely to abate. On the contrary, it is likely to continue to grow, to become more profound, to be tested through litigation and to remain a high priority for legislative attention.[5]

It is no longer a question of legislation or no legislation, but rather of what kind and when. Industry must consider the legal consequences as well as the public effects of its actions—public opinion is a powerful force and must be dealt with accordingly.

---

3. Burrows v. Superior Court, 13 Cal. 3d 238, 529 P.2d 590, 596, 118 Cal. Rptr. 166, 172 (1975) (footnote omitted).

4. *Id.* at —, 529 P.2d at 593, 118 Cal. Rptr. at 169.

5. Fenwick, *Information Technology and Individual Privacy*, THE CREDIT WORLD, April 1975, at 13.

The rising interest of individuals in their right to privacy is illustrated by their desire to have some control over the recordkeeping practices of business and government. Thus, the principal concerns regarding individual privacy today center around

> 1) the desire of the individual to exercise control over the collection of information about himself, including its accuracy, and
>
> 2) the desire of the individual to exercise some measure of control over the use of information about himself once it is collected.[6]

This attitude has gained acceptance as well among high-ranking government administrators. In a speech before the Senate Committee on the Judiciary, former Attorney General Elliot Richardson quoted from a report by the Department of Health, Education and Welfare, saying:

> An individual's personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record. A record containing information about an individual in identifiable form, must therefore, be governed by procedures that afford the individual a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it. Any recording, disclosure, and use of identifiable personal information not governed by such procedures must be prescribed as an unfair information practice unless such recording, disclosure, or use is specifically authorized by law.[7]

Much of the attention of the privacy proponents is focused on the role of computers in the compilation of massive amounts of personal information. However, there are indications that the emotionalism which surrounded the privacy issue a few years ago—particularly in regard to computers—has evolved into a more mature study of the factors involved.[8] Initially, computers were viewed as instruments with a potential for serious abuse; but in recent years—particularly among those well-informed on the privacy issue—the computer has shifted from a position of being inherently suspect to the more neutral role of an

6. See note 2 *supra.*

7. Joint Hearings on *Privacy, the Collection, Use, and Computerization of Personal Data of the Ad Hoc Subcommittee on Privacy and Information Systems of the Senate Committee on Government Operations and the Senate Judiciary Subcommittee on Constitutional Rights,* 93rd Cong., 2d Sess. 36, 53 (1974).

8. See note 5 *supra.*

instrument subject to possible abuse which may be contained by an acceptable variety of means.[9]

There has been however, no concurrent decline in the general fear of compilation of credit information. This fear was caused primarily by the indiscriminate transfer of erroneous credit information, which resulted in such legislation as the Fair Credit Reporting Act.[10] Because of its reputation, the credit industry is looked upon with suspicion. Consequently, the burdens placed upon the credit industry may be greater than those placed upon industry in general:

> A close examination of the competing interests involved in the information environment embraced by a computerized credit system requires a balancing of the exclusion of individuals from the control over the dissemination of their credit information with the effect inclusion would have on commerce. The question now is how to reconcile the legitimate interests of business in this instance in collecting and maintaining personal information with the individual's right to privacy. Though restrictions on the use of credit information might have a negative impact on the profits of credit card activities, could cause some commercial inconvenience by requiring the participation of the cardholder, and could conceivably result in higher service charges to cardholders for the automated account service provided, the such restrictions are essential to securing individual privacy.[11]

If persons were given the right to examine their own record and challenge its accuracy, compilers of credit information would hesitate before including information of questionable validity or placing unfair interpretations upon it.

Computers and credit information are by no means the only objects of such attacks; on the contrary, most of the privacy legislation introduced or proposed would regulate all use of "personal data." "Personal data" is generally defined as including all data that describes anything about an individual; or things done by, or to, an individual, such as records of financial transactions; or that affords a clear basis for inferring personal characteristics or things done by, or to, an individual, such

9. *Id.* One example of this decline in emotionalism is the fact that the word computer is mentioned only three times in the recently enacted Privacy Act of 1974. 5 U.S.C.A. § 552a (Supp. I, Feb. 1975).

10. 15 U.S.C. § 1631 *et seq.* (1970).

11. Comment, *The Privacy Side of the Credit Card*, 23 AM. U.L. REV. 183, 202-03 (1973).

as the mere record of his presence in a place.[12] Under this definition it is hard to imagine any form of record system on individuals which would not be covered.

It is against this background that this comment will examine legislative proposals and trends, on a federal and state level in an attempt to bring some clarity and perhaps forewarning to the business sector in the field of privacy legislation.

II. FEDERAL LEGISLATION

A. HEALTH, EDUCATION AND WELFARE REPORT

In 1971, under then Secretary Elliot Richardson, the Department of Health, Education and Welfare set up a committee to study the automated data systems of the federal government. In 1973, this committee turned in its report,[13] large portions of which were directly incorporated into federal legislation. Because of the report's impact on privacy legislation, it may consequently affect the private sector through either an extension of the federal legislation or by similar incorporation of its concepts into state privacy bills.

B. PRIVACY ACT OF 1974

The Privacy Act of 1974[14] is the legislation enacted by Congress which grew primarily out of the Health, Education and Welfare report. While the Act applies only to the federal government and its agencies, an effort to make certain portions of it applicable to the private sector is gaining momentum.[15] The Privacy Act prohibits or restricts access to records kept by an organization if an individual can be identified with the information contained in those records.[16] Read literally, the requirements of the statute are extremely burdensome, and compliance with them could be expensive.

Following is a brief synopsis of the major requirements of the Act and the difficulties presented should they be extended to the private sector.

---

12. *See* HEW RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973); Penn. H.R. 11, 1975 Sess.

13. HEW RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973).

14. 5 U.S.C.A. § 552a (Supp. I, Feb. 1975).

15. See note 48 *infra* and accompanying text.

16. The law restricts access by those other than the individual on whom the information is kept, but works in conjunction with the Freedom of Information Act, 5 U.S.C. § 552 (1970), to allow the private citizen to have access to the information kept in his file.

Rules Governing Disclosures

The Act prohibits an agency from disclosing information contained in personal records,[17] except with the written consent of the individual to whom the record pertains, unless the disclosure comes within one of eleven exceptions.[18] Under the Act, a record must be made which contains the date, nature, and purpose of each access to the information by any person or agency.[19] This record must also disclose the name and address of those parties who have access to the information, including private citizens as well as agencies.[20] In addition, due to the requirements in the Act concerning notification of erroneous or disputed information,[21] the specific data item accessed must be recorded. Therefore, if the record contained twenty items and seven of them were accessed, a record of each of the items accessed must be kept rather than a mere notation that seven accesses were made. Repeated access must be recorded in the same manner and records of the access must be kept for at least five years or the life of the record whichever is longer.[22] The Act further provides that upon the request of the data subject he must receive an accounting of the accesses made[23] and should any dispute arise as to any of the information contained in the file, the data subject may require that those persons who had access to the information be notified of the dispute.[24]

Individual Access to Records

The information in the records must be made available to the data subject.[25] Thus, an agency is required to locate and identify all of the records containing information about a specific person. These records include correspondence and other noncomputer stored items and would necessarily involve a massive data base and retrieval systems in order to reduce the number of searches required in uncovering all information

17. Disclosure must be read as meaning access, whether on-line or otherwise and whether being printed, displayed on CRT, or simply transferred to another electronic or magnetic medium. *See* Fenwick, *Privacy*, DATA MANAGEMENT, May 1975, at 18.

18. 5 U.S.C.A. § 552a(b) (Supp. I, Feb. 1975). This provision of the statute grants exceptions allowing agencies to make disclosures dealing with ordinary agency use, for criminal law purposes, pursuant to court order, and others.

19. *Id.* § 552a(c)(1)(A).

20. *Id.* § 552a(c)(1)(B).

21. See notes 28 & 29 *infra* and accompanying text.

22. *Id.* § 552a(c)(2).

23. *Id.* § 552a(c)(3).

24. *Id.* § 552a(c)(4).

25. *Id.* § 552a(d)(1).

concerning the individual data subject. The information contained in files as well as daily received information must be placed into the data base to avoid time-consuming and costly file searches.[26] The Act further requires that any information given to a data subject be in a form comprehensible to him.[27] This requirement weakens the efficiency of internal codification of information, which must be decoded before it can be turned over to the individual.

Individual Input into Records

A major purpose of the Act is to allow an individual to dispute the information in his file. Thus, the statute contains provisions allowing the data subject to request a "correction of any portion [of a record] which the individual believes is not accurate, relevant, timely, or complete . . . ."[28] If an agency refuses to amend an individual's record, the individual has a further recourse, and upon his request the agency must "permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement . . . ."[29] The Act also requires the agency to disclose the data subject's statement of dispute whenever access is given to any portion of a record which has been disputed by the individual.[30] This requirement obviously poses massive recordkeeping burdens and problems for an "interactive on-line system."[31]

Notice and Security

Federal agencies are required to publish an annual notice of the existence and nature of each record system covered by the Act[32] and, if necessary, make reasonable efforts to advise individuals that their records have been disclosed pursuant to compulsory legal process.[33] The agency must also establish rules of conduct for those involved in the design, development, operation, or maintenance of a recordkeeping system[34] and must establish safeguards to insure confidentiality (treat-

26. The alternative to such a data file would be a manual system where certain information (for example correspondence) would be kept in actual filing systems requiring large amounts of space and manpower to make physical file searches possible.
27. 5 U.S.C.A. § 552a(d)(1) (Supp. I, Feb. 1975).
28. *Id.* § 552a(d)(2)(B)(i).
29. *Id.* § 552a(d)(3).
30. *Id.* § 552a(d)(4).
31. Fenwick, *supra* note 17, at 19.
32. 5 U.S.C.A. § 552a(e)(4) (Supp. I, Feb. 1975).
33. *Id.* § 552a(e)(8).
34. *Id.* § 552a(e)(9).

ment of personal information once on file) and data security (means of assuring confidentiality).[35]

Privacy Commission

Perhaps the most important provision of the 1974 Act from the business community's view is the creation of a Privacy Commission to study and review the feasibility of making applicable to the private sector the provisions of the Act which currently affect government agencies only. This commission is composed of seven members,[36] three of whom were appointed by the President,[37] two by the President of the Senate,[38] and two by the Speaker of the House.[39]

The commission is empowered to make a study of the information systems of private organizations in order to determine the standards and procedures in force for the protection of personal information.[40] It is to recommend to the President whether the Act should be made applicable to the information practices of private organizations.[41] and may research, examine, and analyze interstate transfer of information about individuals.[42] The commission may conduct hearings, take testimony, and receive evidence under oath, and make use of a subpoena power to compel attendance of witnesses.[43] The ultimate responsibility of the commission is to recommend legislation, administrative action, or voluntary rules it believes necessary to protect the privacy of individuals while meeting legitimate needs for information.[44] It is to report its findings

35. *Id.* § 552a(e)(10).
36. *Id.* § 552a note.
37. The President appointed Willis H. Ware, Senior Computer Specialist at Rand Corp., Santa Monica, California, who headed HEW's Special Advisory Committee on Automated Personal Data Systems, (note 13 *supra*), the group who laid the groundwork for the Privacy Act; William O. Bailey, Executive Vice-President of Aetna Life and Casualty, Hartford, Connecticut; and David F. Linowes, a certified public accountant and partner in the New York City firm of Laventhol & Horwath. A former professor at the University of Illinois, Linowes has been concerned with the problem of balancing the needs of government and private industry for personal information with the individual's right of privacy.
38. Appointed were William Dickinson, the retired executive editor of the Philadelphia Bulletin, and Robert J. Tennesen, a Minnesota State Senator experienced in privacy legislation.
39. Rep. Ed Koch, D-N.Y., and Rep. Barry Goldwater, Jr., R-Calif. were appointed. Representatives Koch and Goldwater sponsored the House version of the Privacy Act of 1974 and they are the sponsors of H.R. 1984 discussed *infra*.
40. Privacy Act of 1974, 5 U.S.C.A. § 552a note (Supp. I, Feb. 1975).
41. *Id.*
42. *Id.*
43. *Id.*
44. *Id.*

within two years of the committee member appointments.[45] During this period members of the business community will have an opportunity to publicize their views to the commission. Thus, it was pointed out in a recent article that

> [t]he time has come for members of the business and industrial communities to take a more active role. [They] should prepare [them]selves to cooperate with, assist and advise the study commission on measures that would avoid unrealistic procedures and limitations, but at the same time would close the door to potential abuse.[46]

The commission must be made aware of relevant factors so it may balance the costs[47] against the social benefits to be gained by regulations in this area.

C. H.R. 1984

House Bill 1984[48] was introduced by Representatives Koch and Goldwater and is primarily designed to extend the protections of the Privacy Act of 1974 to the private sector. The purposes of the bill are set out in section 2(b) which provides:

> (1) There should be no personal information system whose existence is secret.
>
> (2) Information should not be collected unless the need for it has been clearly established in advance.
>
> (3) Information should be appropriate and relevant to the purpose for which it has been collected.
>
> (4) Information should not be obtained by fraudulent or unfair means.
>
> (5) Information should not be used unless it is accurate and current.
>
> (6) There should be a prescribed procedure for an individual to know the existence of information stored about him,

---

45. *Id.*

46. Fenwick, *supra*, note 5, at 15.

47. *E.g.*, impact on routine business transactions, customer convenience, price of commodities.

48. H.R. 1984, 94th Cong., 1st Sess. (1975). Although H.R. 1984 is poorly drafted, it is discussed at length because it is receiving widespread national attention, and an understanding of the personal privacy issue necessarily entails an understanding of the current mood. The second reason for an in-depth look at this bill is the fact that both of its sponsors (Koch and Goldwater) have been appointed to the seven-men Privacy Study Commission established by the 1974 Act. A study of H.R. 1984 should therefore shed light on the opinions of at least two of the members of that Commission. However, the bill, as it now reads, is not likely to be enacted into law. There seems little chance of any more federal legislation being passed in this area until the report of the Privacy Study Commission is received.

> the purpose for which it has been recorded, particulars about its use and dissemination, and to examine that information.
>
> (7) There should be a clearly prescribed procedure for an individual to correct, erase, or amend inaccurate, obsolete, or irrelevant information.
>
> (8) Any organization collecting, maintaining, using, or disseminating personal information should assure its reliability and take precautions to prevent its misuse.
>
> (9) There should be a clearly prescribed procedure for an individual to prevent personal information collected for one purpose from being used for another purpose without his consent.
>
> (10) Federal, State and Local Government should not collect personal information except as expressly authorized by law.[49]

Obviously, the provisions entitling an individual to examine and amend information are designed to strengthen his position in dealing with large organizations rather than to protect his privacy. If the bill was intended solely to protect the right of privacy it would strictly be aimed at the gathering and application of information which may bear negatively upon an individual. But under its current provisions an individual will have access to his file even in the absence of any indication whatsoever that it contains information which may infringe upon his right of privacy. These provisions appear to be aimed at assuring truth and validity in recordkeeping rather than at protecting privacy. Within this framework the general objectives of H.R. 1984 seem to be to inform the public of the existence of recordkeeping systems by notifying each individual within the system, by regulating the collection and dissemination of information so that the information is collected fairly and only if needed, by insuring that the systems are kept current, and by providing civil and criminal penalties for violations. Unfortunately, the bill takes an omnibus approach in an attempt to attain these objectives with one broad piece of legislation.

This omnibus approach creates a number of problem areas within H.R. 1984 which are also common to much of the proposed state privacy legislation. One such area is the lack of sufficient definitions. As drawn, the bill does little to narrow the application of the terms used in it. It is designed to apply to "organizations" but the term "organization" is all-inclusive covering public and private, industrial or commercial entities. Nonprofit and charitable organizations would be within the

49. H.R. 1984, 94th Cong., 1st Sess. § 2(b) (1975).

bill's coverage as it contains no requirement that the "organization" operate for a profit. The general misconception that privacy legislation regulates data banks only is refuted by this privacy bill's application to *every* record system a business or individual businessman may have. Its coverage would extend from a local corner drug store to a national conglomerate, and the relative costs to each would be equally burdensome.[50] The requirement that an organization may use personal information only to accomplish a "proper purpose" of the organization may cause the additional definitional problem of determining the meaning of "proper purpose." After an organization was able to make such a determination it would then face the cumbersome task of reviewing all its files in order to determine whether the material contained therein would fall within the required stated purpose.[51]

In addition to the definitional problem discussed above, the bill would present compliance problems as well. Thus, all stored information would have to be classified in terms of confidentiality requiring a company to review its files and attempt to categorize each piece of data such as correspondence and historical background information in terms of sensitivity. This classification requirement would be extremely burdensome since the sensitivity of information is not static but changes with the circumstances. For example, the age of a data subject would not be sensitive if disclosed to the county coroner but it may very well be if disclosed to a lending institution.[52]

Further requirements of the proposed Act include limitations on dissemination of information to another system or individual unless that system has also complied with the Act, and the transfer is within a stated proper purpose of the organization,[53] and a requirement that an organization maintain a list of all organizations or categories of employees, including identity and purpose, having regular access to personal information in the system.[54] Since access is not defined, a definitional and consequent compliance problem is likely to be encountered. An organization would maintain a record (identity, purpose, and date) of every access to personal information by anyone not having regular access authority.[55] Further, the organization would set up rules for

50. Address by William A. Fenwick, Data Processing Management Association Presents, *A Briefing on the Impact of Privacy Legislation*, Washington, D.C., May 1, 1975.
51. *Id.*
52. *Id.*
53. H.R. 1984, 94th Cong., 1st Sess. § 4(a)(5) (1975).
54. *Id.* § 4(a)(8).
55. *Id.* § 4(a)(9).

compliance and inform all personnel working with such information, or the system, about the requirements of the Act, including penalties prescribed for noncompliance.[56] While a company would be required to implement adequate security measures,[57] the bill does not distinguish administrative, technical, or physical security. Within the proposed Act there is a requirement that any organization dealing in personal information give notice of each system to the Federal Privacy Board[58] and give public notice likely to bring attention of the existence of the records to data subjects.[59] The principle that every personal data file must be licensed, monitored, and policed is impractical because there are approximately twelve million proprietorships, partnerships, and corporations in the United States.[60] Many of them have hundreds of separate personal data files, which means that perhaps as many as 50 or 100 million personal data files would be reported to the government and to the public each year.[61] Furthermore, many of these data files will be changed and expanded, taken out of operation, or replaced by new ones thereby adding to the tremendous reporting load. The notice to the Board and the public would include procedures whereby an individual could determine if he was a data subject, gain access to the information and contest the contents of the record.[62] Organizations maintaining personal information would upon request of any data subject, grant him the right to inspect, in a form comprehensible to him, all personal information about himself, the nature of the sources of the information, and the names of any recipients of the information.[63] These disclosures could be made in person or by mail after proper identification, and if the data subject appeared in person he could be accompanied by another person of his choosing.[64]

The bill sets out procedures for challenging any part of the information. If a dispute were not resolved to an individual's satisfaction he could file a two-hundred-word statement setting forth his position.[65] Thereafter the organization would be required to supply the statement

56. *Id.* § 4(a)(10).
57. *Id.* § 4(a)(11).
58. *Id.* § 7. The Privacy Board would be an administrative body created pursuant to H.R. 1984 to oversee and regulate privacy matters.
59. *Id.* § 4(c).
60. LONG & RUCKER, PERSONAL DATA PRIVACY AND BANKING 8 (1975).
61. *Id.*
62. H.R. 1984, 94th Cong., 1st Sess. § 4(c)(5) (1975).
63. *Id.* § 4(d)(3).
64. *Id.* § 4(d)(4).
65. *Id.* § 4(d)(6)(C).

of dispute in any subsequent dissemination of the disputed information,[66] and upon the data subject's request it would have to notify past recipients of the information of the purging or correction.[67] Such a requirement would impose an undue burden on companies which transfer information on a regular basis without clearly benefiting the data subject as the recipient company would be highly skeptical of the statement of dispute.

The bill would exempt criminal investigation files compiled by federal, state, or local law enforcement organizations.[68] Under this exception, information obtained from a corporation's "in-house" investigative units would not be exempt from the disclosure requirements. This could seriously hamper an "in-house" investigation into criminal activities, since a suspected criminal could gain access to any information gathered about him. For example, a party using a stolen credit card could seek information on file and determine whether the corporation had knowledge of his use of the card and consequently whether it would be safe to continue to use the card or not.

The proposed legislation would also open the employee personnel files of a corporation to its employees. This could effectively eliminate supervisor reports or, at the very least, create a tendency on the part of a supervisor to be less candid with the knowledge that the information could be made available to the employees.

With such legislative language as a background, a number of situations can be imagined in which compliance could prove difficult, if not impossible. Thus, every citizen could approach a corporation and demand to know if a file was kept on him, and if so, its contents. This could prove exceedingly burdensome for any company or industry, which fell into public disfavor and was forced to answer thousands of such inquiries made only for their nuisance value.

Perhaps the most dramatic result of such legislation would be the attendant cost of compliance, which in turn would increase the cost of doing business and, ultimately, would have to be borne by the consumer. A recently completed doctoral thesis projects the cost of compliance with privacy regulations for organizations operating personal data systems.[69] Assuming the accuracy of the projections, they evidence the near

66. *Id.* § 4(d)(6)(D).
67. *Id.* § 4(d)(6)(E).
68. *Id.* § 5(a)(1).
69. Goldstein & Nolan, *Personal Privacy Versus the Corporate Computer*, HARVARD BUSINESS REVIEW, March-April 1975, at 62.

economic impossibility of complying with such legislation. The study included five model personal data systems and projected that cost of compliance for those model systems would range from $142,000 to $1,416,000 in initial conversion costs and from $40,000 to $20,453,000 in annual privacy costs.[70]

III. STATE LEGISLATION

Because of the political popularity of the privacy issue,[71] a total of eighty-five privacy bills were introduced in thirty-six state legislatures during the first half of 1975.[72] At least thirty-four of these bills would apply to the private sector and not merely to public and governmental agencies.[73] Caught in the enthusiasm of the moment these states did not even wait for the members of the Federal Privacy Study Commission to be appointed—much less look at the results of their study—before proceeding to draft their own proposed privacy legislation. It is this irresponsible tendency on the part of legislators to react to politically popular issues which has historically led to regrettable legislation, and may well have that result in this instance. Passage of any significant number of the state bills introduced along with passage of a non-preemptory federal bill could easily result in an unacceptable morass of conflicting requirements on industry. National coherence must exist to arrive at realistic controls in automated data systems which are adequate to protect individual privacy. Proposed state legislation is generally couched in the same language as its federal counterpart, and the means of obtaining the objectives are fairly uniform. Generally these privacy proposals cover three main categories:

A) Controls on operating procedures

> An organization using a personal data system must; take appropriate precautions against natural hazards and other threats to the system and its data, publish descriptions of it periodically, establish procedures for responding to inquiries from individuals about their records and for settling complaints about their accuracy, and keep a log of all uses of each person's record.

---

70. *Id.* at 66.

71. Due to the fact that state legislative action is often patterned after federal legislation, there will necessarily be some duplication of discussion between the portion of this comment aimed at federal privacy action and the part dealing with the actions of the individual states.

72. Metz, *Federal Leadership in Privacy Protection*, 1975 A.B.A.J. 825.

73. Handout entitled *Pending State Privacy Legislation*, distributed by Wm. A. Fenwick, see note 50 *supra*.

B) Access rights of data subjects

A person may; examine his own record, request the correction of any information in it that he believes to be erroneous, and append a statement to the record if the error is not corrected to his satisfaction.

C) Usage control by data subjects

At the time information is collected from someone, he must be told what it will be used for and given the opportunity to refuse to provide it. The subject's permission must again be sought for any new use of the data not covered by his original consent.[74]

The majority of the various state bills contain provisions for public notice of the existence, establishment, or modification of each personal data system. These may include an initial, and annual, registration of the system with some state agency, including a supplemental registration statement when the purpose or use of any personal data system is materially altered from the purpose or use represented in the prior registration statements. There are wide variations in the required contents of such notices, but generally, they require some description of the system, the type of information gathered therein, and the purposes of gathering such information.

While most of the state bills would uniformly regulate certain areas, the minor variations between states would put unreasonable burdens on corporations. For example, most bills would require an organization to record every nonroutine access made. Thus, a bill introduced into the 1975 General Assembly of Pennsylvania[75] would require an organization to "maintain a complete and accurate record of *every access* to, input in, or use made of any and all data in the data system including the identity and address of *any and all* persons and organizations to whom access has been given and the reason for such access, divulgence, transfer, or input."[76] Another requirement of this bill would deny an organization any right to collect on an individual any "information concerning suspicion of . . . a crime . . . ."[77] As previously pointed out, this could prove extremely burdensome for a company which had "in-house" investigative units working on criminal investigations such as credit card misuse.[78]

74. See note 69 *supra*, at 64.
75. H. Bill 11, Pennsylvania, Sess. of 1975.
76. *Id.* § 4(4) (emphasis added).
77. *Id.* § 5(1).
78. See text accompanying note 68 *supra*.

Another area covered in some of the state bills deals with a data subject's access to the courts. Some state bills would allow an individual to have his dispute regarding such matters as accuracy and relevancy of information on file adjudicated by a court of law if no settlement can be reached.[79] Such proceedings could prove to be an immense problem if a large number of individuals took advantage of this opportunity. An organization might well compromise its legitimate position merely to avoid a court battle. The legislation could thus become a license to coerce on the part of the individual.

CONCLUSION

It is obvious that the cost to a corporation of influencing and later complying with fifty different legislative enactments would be unreasonably burdensome. The attendant costs of compliance would be considerably less if sensible national legislation were enacted. National industries cannot be burdened with varying requirements in this area. However, the business community faces a politically popular issue which could infringe on its right to operate a profitable business in a free enterprise system if no positive steps are taken. Foremost among positive actions to be initiated is the promotion of preemptory federal legislation.

There are substantial distinctions between government and business personal data systems as well as between companies which offer personal data as their primary product, and the general business community. Most businesses access and use data only for routine administrative and internal purposes. These distinctions between purpose and use should be recognized in any legislative enactments governing privacy.

In an attempt to adopt reasonable legislation in this area the following proposals would seem to strike the necessary balance between protecting the legitimate privacy concerns of individuals and the equally legitimate concerns of business in protecting their right to profitably remain in operation.[80] First, the law should exempt routine uses, accesses, disclosures, and transfers of data by employees who maintain the records and have legitimate needs for the records in the performance of their duties. Second, personal data should be freely transmitted from an organization to a service bureau when the third party carries out admin-

79. H. Bill 11, § 9(b), Pennsylvania, Sess. of 1975; S. 3178, § 95, New Jersey, Sess. of 1975.

80. Some of the author's proposals are based upon an unpublished, privately contracted study.

istrative activities which would otherwise be performed as a normal and unrestricted function of the business, and there should be no requirement of notice to or consent from the data subject so long as only routine use is made of the data. Third, the security required by law to protect the privacy or records should consider the sensitivity of the data and the technical feasibility of compliance in the organization. Fourth, the organizations should be statutorily protected from mere harrassment by limiting the hours of access, permitting a reasonable fee to be charged per access and limiting the number of annual accesses unless a significant change has occurred in a file. Fifth, the laws should exempt those routine uses of personal data within the concept of normal business practices, so long as the data is not used in a manner which could not reasonably be expected by the data subject considering his relationship to the organization.

A balance must be achieved, and these suggested guidelines would not violate the individual's right to privacy while at the same time avoiding the undesireable disruption of business activities.

Charles W. Pauly