45665

AD/A-022 186

COST IMPLICATIONS OF PRIVACY PROTECTION IN DATABANK SYSTEMS

REIN TURN

RAND CORPORATION
SANTA MONICA, CALIFORNIA

APRIL 1975

KEEP UP TO DATE

Between the time you ordered this report—which is only one of the hundreds of thousands in the NTIS information collection available to you—and the time you are reading this message, several *new* reports relevant to your interests probably have entered the collection.

Subscribe to the **Weekly Government Abstracts** series that will bring you summaries of new reports *as soon as they are received by NTIS* from the originators of the research. The WGA's are an NTIS weekly newsletter service covering the most recent research findings in 25 areas of industrial, technological, and sociological interest—invaluable information for executives and professionals who must keep up to date.

The executive and professional information service provided by NTIS in the **Weekly Government Abstracts** newsletters will give you thorough and comprehensive coverage of government-conducted or sponsored research activities. And you'll get this important information within two weeks of the time it's released by originating agencies.

WGA newsletters are computer produced and electronically photocomposed to slash the time gap between the release of a report and its availability. You can learn about technical innovations immediately—and use them in the most meaningful and productive ways possible for your organization. Please request NTIS-PR-205/PCW for more information.

The weekly newsletter series will keep you current. But *learn what you have missed in the past* by ordering a computer **NTISearch** of all the research reports in your area of interest, dating as far back as 1964, if you wish. Please request NTIS-PR-186/PCN for more information.

WRITE: Managing Editor
5285 Port Royal Road
Springfield, VA 22161

Keep Up To Date With SRIM

SRIM (Selected Research in Microfiche) provides you with regular, automatic distribution of the complete texts of NTIS research reports *only* in the subject areas you select. SRIM covers almost all Government research reports by subject area and/or the originating Federal or local government agency. You may subscribe by any category or subcategory of our WGA **(Weekly Government Abstracts)** or **Government Reports Announcements and Index** categories, or to the reports issued by a particular agency such as the Department of Defense, Federal Energy Administration, or Environmental Protection Agency. Other options that will give you greater selectivity are available on request.

The cost of SRIM service is only 45¢ domestic (60¢ foreign) for each complete microfiched report. Your SRIM service begins as soon as your order is received and processed and you will receive biweekly shipments thereafter. If you wish, your service will be backdated to furnish you microfiche of reports issued earlier.

Because of contractual arrangements with several Special Technology Groups, not all NTIS reports are distributed in the SRIM program. You will receive a notice in your microfiche shipments identifying the exceptionally priced reports not available through SRIM.

A deposit account with NTIS is required before this service can be initiated. If you have specific questions concerning this service, please call (703) 451-1558, or write NTIS, attention SRIM Product Manager.

This information product distributed by

NTIS U.S. DEPARTMENT OF COMMERCE
National Technical Information Service
5285 Port Royal Road
Springfield, Virginia 22161

COST IMPLICATIONS OF PRIVACY PROTECTION IN DATABANK SYSTEMS

Rein Turn

April 1975

P-5321

COST IMPLICATIONS OF PRIVACY PROTECTION IN DATABANK SYSTEMS

by Rein Turn
The Rand Corporation
Santa Monica, California

INTRODUCTION

The last ten years in the development of computerized personal information databank systems in the United States, and a somewhat shorter time period in other North American and Western European countries, have seen a mounting concern over the violations of privacy and other individual rights of the data subjects that may result from the use of such systems. In the United States a series of Congressional hearings, articles in professional and popular journals[1,2], and the reports by the National Academy of Sciences (NAS) project on databanks[3], and the Advisory Committee on Personal Data Systems of the Secretary of Health, Education and Welfare (HEW)[4] culminated in the enactment of the federal Privacy Act of 1974[5]. This Act applies to all record-keeping systems maintained by the Federal Government. Similar laws have been proposed in nearly all of the States and some have been enacted (e.g., in Minnesota[6]). New legislation has been introduced in Congress[7] to extend privacy protection requirements also to state and local governments, and to the public sector.

At the same time, important reports on safeguarding privacy were issued in Canada[8] and in the United Kingdom[9], and the first national privacy protection law, the Swedish Data Act[10], went into effect in July 1973. Preceding the Swedish Data Act, the Land Hessen of the German Federal Republic had enacted a Data Protection Act[11] in October 1970, and the Fair Credit Reporting Act of the United States[12], effective since April 1971, had instituted a set of privacy protection requirements for a limited albeit pervasive class of personal information record-keeping systems--those operated by, or for the purposes of, consumer credit granting institutions and business.

The purpose of the enacted and the pending privacy protection legislation is to establish requirements on personal information databank systems to assure that privacy and other individual rights of the data subjects are not violated or unduly restricted. These requirements take many forms, can be implemented in various ways, and have different technical and economic implications on all organizations. Indeed, most of the safeguards proposed have not been analyzed from the point of view of their economic implications--the initial costs of their implementation and the recurrent costs of their operational use.

This paper categorizes the proposed safeguards, examines alternative ways of their implementation, and discusses the

cost implications. The analysis is mostly qualitative, since actual cost data are difficult to obtain--the only sources of such information are private institutions now operating under the privacy requirements of the Fair Credit Reporting Act and estimates by various organizations of the costs of complying with the requirements of pending privacy legislation[13]. The former tend to be proprietary, the latter are often grossly inflated to discourage enactment of the privacy legislation.

PRIVACY PROTECTION

In the context of personal information databank systems, the term "privacy" is being used to represent a set of the rights relative to personal information of an individual data subject on whom identifiable personal data are being maintained in a databank system, regarding the collection, storage, processing, dissemination and use of information on his personal attributes and activities. These rights are based on the following fundamental principles expressed in the Code of Fair Information Practices[5]:

1. There must be no personal data record-keeping system whose very existence is secret.
2. There must be a way for an individual to find out what information about him is in a record and how it is used.
3. There must be a way for an individual to correct or amend a record of identifiable information about him.
4. There must be a way for an individual to prevent information about him that was obtained for one purpose to be used or made available for other purposes without his consent.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

These principles form a basis for the definition of specific rights afforded to the individual data subjects, and specific protection requirements to be placed on organizations that maintain personal information databank systems. Such rights and requirements are stated in the Code of Fair Information Practices and adopted in the privacy protection legislation already enacted or still pending, in particular in the Privacy Act of 1974.

Fundamental in establishing individual rights and protection requirements are the designation of one official as responsible for the databank system(s) maintained by his organization, and the annual issuance of an official public statement on every databank system and its functions. The required statement includes the following information: the name and location of the databank, and identification of the responsible official; and for each separate system of records in the databank, (1) the categories of individuals on whom records are maintained, (2) the categories of information items in the records, (3) the purposes for which the information items are used, (4) the categories of employees of the organization who use the records for stated purposes, and (5) the names of other organizations to whom information from the databank is disseminated for the stated purpose along with categories of information so disseminated. The above statement defines the routine purposes, use, users, and dissemination practices of the organization. The statement is also required to describe the policies and practices of the organization regarding storage, retrievability, retention, and disposal of the records, and the procedures used for controlling access, assuring data integrity, and permitting individual data subjects to exercise their rights.

The rights of individual data subjects fall into the following general categories. The specifics will be discussed

later in this paper.

- o Notification. The right of an individual to know about the existence of all personal files on him, the routine uses of these data, any non-routine actions that may have been made or are pending.
- o Access. The right of the data subject (or his designated representative) to inspect his own files, presented in humanly readable and intelligible form, and to obtain copies of these files.
- o Correction and Amendment. The right to challenge the veracity, relevance, accuracy, pertinence and completeness of his personal file; the right to request correction or removal of information items in the personal file, and to submit supplemental or rebuttal material.
- o Control. The requirement on the databank-keeping organization to request the data subject's consent for collecting certain information (e.g., on religious belief or political views), or taking non-routine actions regarding his personal file.
- o Assurance of Compliance. The requirements on the databank-keeping organization to implement techniques and procedures that assure that the individual data subjects' rights are upheld, including the proper performing of the functions for which data are kept (for example, providing benefits for

the data subjects). This includes implementing procedures for computer security, controlling access to the files, maintaining data integrity, and taking steps to prevent loss of data or interruption of the services provided. Various penalties are specified in pending legislation for willful non-compliance with the protection requirements or denial of an individual data subject's rights, as well as for attempts by anyone to access, use, and modify the data files in some unauthorized ways.

- o Redress. The right of an individual data subject to demand compensation for damages that he may have suffered because of the failure of a databank-keeping organization to comply with the protection requirements.

The major classification dimensions of personal information databank systems are[4,14]: the nature of the organization that maintains the databank--public or private; the main purpose of maintaining the databank--administrative, statistical reporting and research, and intelligence and investigative; and the way that the files are maintained--manual or computerized. With certain exceptions, the privacy protection principles stated above are applicable to all of these databank classes. For example, personal information in databanks used purely for statistical reporting or research is not used to make decisions on specific individuals and, therefore, there is no need for correction or rebuttal,

but strong safeguards must be established to prevent use of such information for any other purpose and to control dissemination of such information in identifiable form [4]. Exemptions are also being granted (e.g., in the Privacy Act of 1974) for investigative databanks (e.g., those maintained intelligence operation of the Federal government and by law enforcement agencies) on grounds that investigative work would be severely hampered if individuals under early investigation were aware of it and could follow the progress of investigations by inspecting their files.

IMPLEMENTATION CHOICES AND COST IMPLICATIONS

There are a number of ways for specifying the details of the rights afforded to individual data subjects, and a variety of technical means for their implementation in different classes of databank systems. As may be expected, the costs involved depend on the specifics of the requirements and on the choice of implementation. Indeed, protection requirements may be legislated in forms that make their implementation exceedingly costly. For example, the earlier proposals for the Privacy Act of 1974 also applied to the manual records kept in the National Archives. The cost of notification of the data subjects or their next of kin of the existence of records was estimated to exceed one billion dollars. It is hoped that in this section the analysis of cost implications of the various choices in meeting privacy protection requirements can be used as a framework for making

specific protection requirements and choosing ways for their implementation.

Cost elements

As in any system, the costs of implementing privacy protection requirements in personal information databank systems comprise the initial costs of setting up the protection system, and the recurrent operational costs. Typical among initial costs are those incurred in:

- Analyses of the impact of the specific protection requirements on the databank system and designing plans for complying with the requirements.
- Design and implementation of policies, procedures and regulations for implementing a selected protection system.
- Acquisition of protection-oriented equipment and facilities, improving the system's physical security, setting up mechanisms for interacting with data subjects, and setting up protection-oriented record-keeping systems.
- Generation, validation and testing of protection-oriented system's software and data base management programs; modification of existing systems and applications programs. If necessary, conversion of the data base formats to include information necessary for complying with protection requirements.

The credit reporting industry's experience with implementing the requirements of the Fair Credit Reporting Act (FCRA) has shown that preparation for handling data subjects' inspection and correction requests is one of the major initial cost items. For example, after the passage of the FCRA, the annual number of inspection requests received by TRW Credit Data Corporation[15] increased by a factor of one thousand--from 2000 to 200,000 a year. This necessitated the establishment and staffing of special departments at all branch offices, at an annual cost of some $2 million. The start-up costs for the Federal databank systems of the Privacy Act of 1974 have been estimated to be of the order of $100 million, and the corresponding annual operational costs in the range of $200 to $300 million[16].

The operational costs of providing privacy protection include the following:

- o Salaries of employees performing protection-related duties, such as interacting with data subjects who are exercising their rights, performing internal auditing functions to assure compliance, operating employee educational programs related to protection, security guards, and the like.
- o Rental and maintenance costs of security-related hardware, such as additional magnetic tape units for recording transaction logs, special display terminals and printers for interacting with data

subjects, anti-intrusion systems, and additional facilities and offices.

- o Communications costs for data links, telephone and mail; costs of expendable materials associated with such communications, such as production of hard copy of data subjects' records.
- o Computer time for access and dissemination control, maintaining transaction logs and audit trails, retrieving records for inspection by data subjects and for augmenting individual records.
- o Storage space in on-line and off-line memory devices needed for adding protection-related data fields to individual records, protection-related programs, and for transaction logs and audit trails.

Some of the protection-related operational costs can be expected to be distributed throughout the databank operations in the form of additional security precautions, reduced availability of the system and data files, reduction in employees who are permitted access, and more stringent controls over the use of personal information for the purposes of the databank-keeping operation. The effect will be a reduction of the system's availability, throughput and efficiency. In this respect the implementation of privacy protection safeguards will be in conflict with the traditional goals of the system's manager, and users. If

these reductions are large, the databank system may be unable to meet its peak inquiry-handling or processing demand and may need additional processors or faster processors, additional on-line storage and capacity.

That part of the operating costs involving inspection requests by individual data subjects can be expected to be stochastic in nature--an initial surge of requests at the inception of the privacy protection legislation will settle to a lower level of requests which will fluctuate on the national level, regionally or locally, and will fluctuate in different types of databank systems as a function of events that take place in politics, legislation, economy, etc. For example, in the credit reporting industry the inspection request rate is coupled to the lending policies of financial institutions--as credit tightens, loans are harder to get, lending agencies become more selective, and the increased rate of credit refusals brings an increased number of credit record inspection requests.

The annual privacy-related operating costs have been estimated by organizations in private sector to be in the $0.57-$6.97 range per data subject, and in the $0.15-$3.93 range per transaction[13].

Notification

In compliance with an individual data subject's right to know, the privacy protection legislation is likely to contain requirements for notification of the general public, and individual notification of data subjects. Public notices will be required to completely describe the routine purposes, data files, and data uses of the databank. The notice will have to be submitted

to a government agency charged with controlling databanks, and published in some official journal (e.g., Federal Register). Also required may be the publication of a privacy impact statement which describes the consequences to the individual of the databank system and its use[17]. The preparation of the first such public notice is likely to entail considerable personnel time.

The databank-keeping organization will be required to notify a data subject individually of several or all of the following: (1) existence of a file on him, (2) initiation of a legal process to force disclosure of his file, (3) reactivation of an archival file on him, (4) requests for non-routine use or dissemination of his file, (5) any disclosure made of his file, (6) whether or not he is legally required to produce additional data that are requested. Some of these notifications may be required only when a data subject submits a request, others may have to be issued automatically to all data subjects at the same time, or to individual data subjects when a file is set up and other mentioned situations arise.

The unit cost of an individual notification is essentially that of the postage for mailing the notification. The cost of preparing the notification letter itself is comparable to that of computerized preparation of address labels and simple billings. Indeed, if the databank-keeping organization is in routine contact with the data subjects, a number of notification requirements may be handled as part of such routine mailings. A

statement about the legal requirement to give information can be printed on the questionnaire forms.

In cases where separate mailings must be made, the total cost is proportional to the volume of notifications and can be substantial if the data subject must be notified of each access in a highly active databank system. For example, in 1973 the National Crime Information Center (NCIC) handled nearly 40 million transactions, and the daily inquiry rates in commercial credit reporting agencies may approach 80,000 to 100,000. The cost per record-existence notification has been estimated in the $0.09-0.048 range[13].

The databank must also maintain transaction logs for recording the dates and modes of notifications such that they are individually retrievable for auditing and inspection. A six-byte data field should be sufficient for each individualized notification. Information on mass notification could be maintained in manual records. Legislation may require that notification data be maintained for several years.

Inspection, correction and amendments

The right of individuals to inspect their personal files means that a data subject must be allowed, with some exceptions, to examine visually a comprehensible copy of his file in person at a databank location, request assistance in interpreting his file, or request a copy by mail. For this purpose, the databank-keeping organization may be required to "define

reasonable items, places, and requirements for identifying individuals who request records pertaining to themselves."

In particular, the individual data subject may be given the rights to access several or all of the following categories of information in his personal file or pertaining to his file: (1) tne contents of his file in comprehensible form (except certain medical and psychological records for which special procedures would be set up, and other information which may be specifically exempted); (2) the nature of sources of information, (3) the identities of non-routine recipients or users of information from his file.

The rights to challenge, correct, supplement, and enter a rebuttal require that the databank-keeping organization (1) establish procedures for reviewing challenged information items, (2) make the corrections requested by the data subjects or inform him promptly of refusal to amend and the reasons thereof, (3) permit the data subject to supplement his file with a concise statement on the disputed information items and the reasons of dispute, (4) include the rebuttal statement and the organization's reason for refusing the data subject's correction, and (5) notify prior recipients of a corrected record of the corrections made.

The operational costs of providing for these data subjects' rights include the facilities, equipment and salaries of a "customer relations" department set up to handle the inspection requests, verify submitted supplemental information, and help in

the preparation of rebuttal statements. Computer time will be used for retrieval of personal files and their decoding into a narrative form (typically replacing two- or three-character codes with sentences explaining their meanings, and describing the meaning of all numerical entries). This expansion can easily reach 10 to 1,or more. Inspections at databank offices must be handled during prime shift working hours and, thus, add to the workload. Other inspection requests have more flexibility for their processing. Additional processing time is required for amending personal files.

Experience with the Fair Credit Reporting Act provides one data point by showing[15] that inspection requests are likely to be less than .3 percent of the annual inquiry volume, that (at least initially) modifications of personal files are made in about one-third of the inspected files, and that cost per customer interaction is about $8. A part of that, the cost of preparing a copy of the file, may be charged to the individual.

Additional data fields must be provided in disputed personal files for rebuttal statements and explanations by the databank, or for linkage to some other part of the on-line storage where such statements are stored. Some pending bills have specified a 200 word limit of the rebuttal statement[7], and others specify that the statement be "of reasonable length" or "concise." Further data fields are required to store the date, means, and results of each interaction with a data subject.

Transaction logs must be kept on all accesses to personal files in order to be able to notify prior recipients of corrections that may have to be made in the future. The time period for which transactions must be stored is two years in the Privacy Act of 1974 and in the Fair Credit Reporting Act, but specified only as "reasonable time period" in others.

Consent and control

The requirements to obtain a prior written consent of a data subject may apply to (1) requests by other organizations for non-routine transfers of personal files, (2) requests to transfer personal files beyond the borders of the country, and (3) collection of certain personal information, such as religious and political views. In addition, commercial credit reporting agencies are required to obtain the individual's consent before initiating an investigative report on the individual.

The costs of obtaining the written consent are essentially the same as sending notification: postage for letters requesting the consent, and data fields for recording the data consent if given or refused.

Requirements to assure compliance

To assure that the individual rights provisions are implemented, the Code of Fair Information Practices, the Privacy Act of 1974, and the pending legislation in Federal and state levels establishes a number of additional requirements. Depending on the particular legislation, a databank may have to satisfy all or some

subset of the following:

(1) Collect, maintain, use, and disseminate only such personal information as is necessary to accomplish the proper purpose of the organization;

(2) Maintain personal information with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness of any decision made on the basis of the personal information;

(3) Establish a sensitivity classification for personal information to be used in conjunction with confidentiality requirements and access controls;

(4) Take precautions to assure that only authorized employees of the databank-keeping organization, and of user organizations, are afforded access to the personal information files;

(5) Take precautions to protect the databank system and data files from any anticipated threats or hazards, and establish appropriate security safeguards;

(6) In statistical reporting databanks, release no individually identified personal information, or statistical summaries that can be traced back to individuals through statistical disclosure.

(7) Establish rules of conduct and inform each person involved in the design, development, operation, or maintenance of the databank system about the legal

requirements to safeguard data subjects' rights, prevent unauthorized access, and provide security.

Finally, penalties are specified for willful violation of the privacy protection requirements, attempts to obtain unauthorized access, and for negligent operation of the system. The data subjects are given the right to file civil actions against the databank and seek redress and remedies for actual damages, and demand punitive damages.

To comply with the first three requirements, an organization must perform a thorough analysis of its purposes and information needs. Standards may be needed for sensitivity classification of personal information[14,19], and for commensurate levels of protection. Retention standards may have to be developed for different information categories to meet the timeliness requirements, and provisions made in personal files to store "confidentiality tags" and age information on selected information items. Standard data integrity techniques, such as check-sums[20] may have to be used to detect accidental or unauthorized modifications of individual files.

The fourth and fifth requirements in the above list represent the need for <u>controlled accessibility</u> in the on-line data files, and <u>security</u> safeguards at all locations within the organization where personal information is handled or processed. The design and implementation of controlled accessibility in the computer operating system software of a

modern multiuser, resource-sharing, remotely accessible computer system where there exist threats of unauthorized access by "malicious users," is a complex task not yet totally understood. Thus, no existing operating system is regarded as absolutely secure against determined intrusion attacks. In less complex systems, such as databanks where the users are restricted to using a system-provided query language for information retrieval, and where effective procedures have been established for the identification of authorized users, threats of unauthorized access can be greatly reduced. However, it is not within the scope of this paper to discuss controlled accessibility or physical security in detail. The reader is referred to recent publications on these topics[21-23].

The costs of controlled accessibility and physical security include the initial costs of designing, implementing and testing the access-control features in the system's software, and acquiring hardware for the security system. The operational costs include: (1) computer time for user identification and authentication, and application of access-control tests by the file management system; and (2) storage space for the access-control program modules, tables, and data fields. In general, it is estimated[21,23] that access-control features in a system's software tend to increase the overall processing time by 5 to 10 percent, the operating

system's software by 10 percent, and the memory requirements for the operating system's use by 10 to 20 percent.

Finally, the liability of the databank-keeping organization for damages suffered by data subjects through non-compliance or negligence of the organization's employees, and the criminal penalties that may be applied, require the setting up of a legal department and an internal security department to enforce security procedures and rules, and apply internal discipline. An internal auditing department should also be established to test and evaluate the effectiveness of the access-control and security safeguards, and the procedures for interacting with data subjects.

SUMMARY

Legislation is now pending in the United States and other countries, on national as well as local levels, to codify various rights that individual citizens have relative to personal information stored on them in computerized databank systems. The pending legislative proposals establish specific requirements to be implemented by the databank-keeping organizations. A qualitative analysis of the cost factors associated with the implementation of these requirements shows that: (1) it may be possible to satisfy notification requirements in the course of regular communications from the databank organization to the data subjects; (2) special personnel, equipment and facilities will be required to

satisfy data subjects' inspection reques s, review disputed data items, handle personal security, and enforce internal procedures and rules; (3) detailed transaction logs must be set up and transaction records maintained for periods as long as five years; (4) new data fields may be needed in personal files to record information on various interactions of data subjects with the databank-keeping organization, the age and sensitivity of certain data items, supplemental information or rebuttal statements submitted by the individual, and pointers to transaction histories that identify past users and uses of the subject's personal file; (5) a relatively modest amount of computer time will be required for handling the more routine interactions with data subjects; (6) computer time and storage space will be required for identification and access-control programs. In summary, the limited experience with the implementation of Fair Credit Reporting Act privacy protection requirements shows that these costs tend to be relatively minor when compared to the routine operating costs of databank systems.

REFERENCES

1. Hunt, M. K. and R. Turn, Privacy and Security in Databank Systems: An Annotated Bibliography, 1970-1973, R-1361-NSF, The Rand Corporation, Santa Monica, California, March 1973.

2. Federal Data Banks and Constitutional Rights, United States Senate, Subcommittee on Constitutional Rights of the Committee on the Judiciary, 93d Congress, 2nd Session, Washington, D.C., 1974.

3. Westin, A. F. and M. A. Baker, Databanks in a Free Society, Quadrangle Books, New York, N.Y., 1972.

4. Records, Computers, and the Rights of Citizens, A Report of the Secretary's Advisory Committee on Automated Personal Data Systems. U.S. Department of Health, Education, and Welfare, July 1973. DHEW Publication No. (OS) 73-94.

5. Privacy Act of 1974, Title 5, United States Code, Section 552 a (Public Law 93-579), December 31, 1974.

6. "Minnesota Data Security and Privacy Act," Minnesota Session Laws 1974, Chapter 479, 1974.

7. Comprehensive Right of Privacy Act, Bill H.R. 1974, U.S. Congress, House of Representatives, January 23, 1974.

8. Privacy and Computers, Task Force Report, Departments of Communication and Justice, Information Canada, Ottawa, 1972.

9. Report of the Committee on Privacy, Secretary of State of the Home Department, Her Majesty's Printing Office, London, July 1972.

10. "Sweden Enacts Privacy Law," Electronics, July 19, 1973, pp. 72-73.

11. Gassman, H. P., "Databanks and Individual Privacy: The Situation in the German Federal Republic," Computer Communications: Impact and Implications (S. Winkler, Ed.),

Proceedings, First International Conference on Computer Communications, Washington, D.C., October 24-26, 1972, pp. 108-113.

12. "Protecting Privacy in Credit Reporting," Stanford Law Review, February 1972, pp. 550-567.

13. Goldstein, R. C. and R. L. Nolan, "Personal Privacy Versus the Corporate Computer," Harvard Business Review, March/April 1975, pp. 62-70.

14. Turn, R., Privacy and Security in Personal Information Databank Systems, R-1044-NSF, The Rand Corporation, Santa Monica, California, March 1974.

15. "Definition of Privacy Needed Before Action Can Start," Computerworld, May 15, 1974, p.6.

16. Privacy Act of 1974, A Report to Accompany H.R. 16373, Report No. 93-1416, United States House of Representatives, 93d Congress, 2nd Session, Washington, D.C., October 2, 1974.

17. Government Data Bank Right to Privacy Act, A Bill, S.3633, United States Senate, 93d Congress, 2nd Session, June 12, 1974.

18. California Fair Information Practice Act of 1973, Assembly Bill No. 2656, California State Assembly, Sacramento, California, January 7, 1974.

19. Bing, Jon, "Classification of Personal Information With Respect to the Sensitivity Aspect," Databanks and Society, Proceedings of the First International Oslo Symposium on Data Banks and Society, Universitetforlaget, Oslo, 1972, pp. 98-150.

20. Martin, J., Security, Accuracy, and Privacy in Computer Systems, Prentice-Hall, Inc., Englewood Cliffs, N.J. 1973.

21. Data Security and Data Processing, Vol. 1-6, IBM Corporation, White Plains, N.Y., June 1974.

22. Guidelines for Automatic Data Processing: Physical Security and Risk Management, FIPS Pub. 31, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., June 1974.

23. Weissman, C., "Security Controls in the SDEPT-50 Time-Sharing System," AFIPS Conference Proceedings, Vol.35, 1969 Fall Joint Computer Conference, pp. 119-133.

END