DOCUMENT RESUME

ED 144 539 IR 004 959

AUTHOR Fong, Elizabeth
TITLE Computer Science and Technology: A Data Base Management Approach to Privacy Act Compliance.
INSTITUTION National Bureau of Standards (DOC), Washington, D.C. Inst. for Computer Sciences and Technology.
REPORT NO NBS-SP-500-10
PUB DATE Jun 77
NOTE 39p.; Computer Science and Technology Series; For related document, see IR 005 072
AVAILABLE FROM Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402 (C13.10:500-10, Stock no. 003-003-01787-6, $1.40)

EDRS PRICE MF-$0.83 HC-$2.06 Plus Postage.
DESCRIPTORS *Agencies; Automation; Civil Liberties; Computer Programs; *Confidentiality; *Confidential Records; *Data Bases; Information Systems; Privacy; *Program Development; Standards
IDENTIFIERS *Data Base Management; *Privacy Act 1974

ABSTRACT

The Privacy Act of 1974 (PL 93-579) and guidelines for its implementation impose requirements on Federal agency personal record-keeping practices. This report presents an implementation strategy for the administration of certain Privacy Act requirements with the use of current data base management systems. These requirements are analyzed in the light of data base software functional characteristics, and implementation approaches utilizing commonly available data base management systems are described. As these approaches cannot anticipate every possible situation, they should not be construed as an official standard or legal interpretation regarding the Act's provisions. Rather, they provide tools for efficient and effective computer utilization in Privacy Act compliance by extending routine processing functions to include necessary administrative functions at minimal additional cost. Appendices include references, a summary of requirements of the Act, and tables listing correlations with compliance procedures and data base management system functions for the requirements of data collection, maintenance and use; access; amendment; dispute handling; disclosure; and public notice. (Author/KP)

COMPUTER SCIENCE & TECHNOLOGY:

A Data Base Management Approach to Privacy Act Compliance

Elizabeth Fong

Systems and Software Divisio.
Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D.C. 20234

U.S. DEPARTMENT OF COMMERCE, Juanita M. Kreps, Secretary
Dr. Sidney Harman, Under Secretary
Jordan J. Baruch, Assistant Secretary for Science and Technology
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, Acting Director

Issued June 1977

Reports on Computer Science and Technology

The National Bureau of Standards has a special responsibility within the Federal Government for computer science and technology activities. The programs of the NBS Institute for Computer Sciences and Technology are designed to provide ADP standards, guidelines, and technical advisory services to improve the effectiveness of computer utilization in the Federal sector, and to perform appropriate research and development efforts as foundation for such activities and programs. This publication series will report these NBS efforts to the Federal computer community as well as to interested specialists in the academic and private sectors. Those wishing to receive notices of publications in this series should complete and return the form at the end of this publication.

National Bureau of Standards Special Publication 500-10
Nat. Bur. Stand. (U.S.), Spec. Publ. 500-10, 34 pages (June 1977)
CODEN: XNBSAV

Library of Congress Catalog Card Number: 77-608106

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1977

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402 - Price $1.40
Stock No. 003-003-01787-6

PREFACE

The Privacy Act of 1974 (PL 93-579) and OMB guidelines for its implementation impose requirements on Federal agency personal record-keeping practices. This report presents an implementation strategy for the administration of certain Privacy Act requirements with the use of today's data base management systems. These Privacy Act requirements are analyzed in the light of data base software functional characteristics, and implementation approaches utilizing commonly available data base management systems are described. As these approaches cannot anticipate every possible situation, they should not be construed as an official compliance standard or legal interpretation regarding the Act's provisions. Rather, they provide tools for efficient and effective computer utilization in Privacy Act compliance by extending routine processing functions to include necessary administrative functions at minimal additional cost.

ACKNOWLEDGEMENTS

The author would like to express her thanks for the technical contribution given by Mr. I. Trotter Hardy of National Bureau of Standards in the preparation of Appendix I, Privacy Act requirements analysis. Thanks go to Dr. Thomas C. Lowe of National Bureau of Standards who gave incentive and direction throughout the course of this work. Thanks also goes to Dr. Dennis W. Fife, and Mr. John L. Berg of National Bureau of Standards for their constructive review of this report.

TABLE OF CONTENTS

Page

A DATA BASE MANAGEMENT APPROACH TO PRIVACY ACT COMPLIANCE

Elizabeth Fong

The Privacy Act (PL 93-579) provisions on personal record handling present new issues concerning effective use of commercial data base management systems (DBMS) by Federal agencies. The widespread use of such systems in record-keeping activities will definitely have an impact on methods of administering compliance with the Privacy Act. This report proposes a technical approach to compliance with certain Privacy Act requirements through the use of generalized data base management system. Requirements are translated into a set of computer data file and procedures. These procedures, incorporated at pivotal points of data base software, can implement those Privacy Act compliance procedures amenable to automation. The use of DBMS appears to be a viable and technologically feasible solution to the effective and efficient implementation of many Privacy Act provisions.

Key words: Computer utilization; data base functions; data base management systems; Privacy Act of 1974; privacy compliance techniques.

1. INTRODUCTION

Data Base Management Systems (DBMS) provide the technology which makes it possible to administer vast record-keeping on an efficient basis. Large computer files of several million records now are used in all but the smallest enterprises to provide current status information and timely management for personnel, inventories, property, financial accounts, and other functions. Thus, data base management systems are a key area for implementation of procedures and safeguards to protect privacy and facilitate compliance with legislation.

The Privacy Act of 1974 (PL 93-579) [1] sets forth requirements governing Federal agency personnel record-keeping practices. The key to the Privacy Act administration is the establishment of policies which control the use of personal data. The requirements imply that certain data usage and dissemination be monitored and controlled. The Privacy Act provisions on personal record handling give rise to issues concerning effective use of commercial data base management systems by Federal agencies. The increasing use of DBMS by agencies in their data processing to support their missions raises the question of how DBMS capabilities can be advantageously used to aid the administration of Privacy Act requirements.

1.1 Motivation

NBS experience shows that agencies' current compliance procedures are typically manual. The questions that arise from this observation are (1) whether compliance procedures are amenable to automation; and (2) if so, whether these procedures should be incorporated in a generalized data base management system.

The two questions imply management decisions that are to some extent unique to each agency. Nevertheless, some guidance can be given on what the possibilities are for using a DBMS to implement provisions of the Privacy Act. This report is addressed to agencies (1) that are presently using computers for record storage, and (2) that either possess a DBMS, or consider the future acquisition of a DBMS to be a distinct possibility. If the agency is in this situation, this report should aid in its efforts to comply with the Privacy Act and to determine what DBMS capabilities can be advantageously used.

The report is aimed, in particular, at data base administrators or data base managers. Those agencies with an existing DBMS can expect to learn what their system can do in complying with the Act, and what ways of using the DBMS to implement the Act's provisions are most likely to be feasible. For those agencies without an existing DBMS, this study can point out in what ways a DBMS could help them in implementing requirements of the Privacy Act.

1.2 Scope

The scope of this study is limited to those compliance requirements with the Privacy Act which we judge to be good candidates for automation by means of a data base management system. For official guidance on specific instructions on compliance, the reader is directed to several relevant documents [2,3,4]. The OMB Circular No. A-108 [2] defines responsibilities for implementing the Privacy Act. Bushkin [5] provides a reference manual for compliance with the Act.

In the proceedings of a workshop "Data Base Directions - The Next/Step" [6], the section on "Impact of Government Regulations" assesses the impact of regulations on data base system functions. Compliance requirements mentioned in this report are taken from all of the above mentioned documents.

Physical security and "appropriate safeguards" aspects are treated in FIPS PUB 41 [4], and will not be covered in this study. The security aspects involving accidential or intentional disclosure to unauthorized persons are not directly addressed.

For the purpose of this study, a DBMS is characterized as a generalized software package, which provides a single flexible facility for accommodating different data files and operations while demanding less programming effort than conventional programming languages, e.g., COBOL. DBMS software possesses the following general properties:

- It facilitates operation on data such as data definition, data storage, data maintenance, data retrieval, and output.
- It facilitates reference to data by name and not by physical location.
- It operates in a software environment which is not tied to a particular set of application programs or files.

It is also assumed that the data base contains data constituting all or part of a "system of records," as defined in the Privacy Act.

1.3 Approach

The overall approach in this report is to gather two different sets of data for analysis. These data are:

- Privacy Act requirements translated into compliance procedures that could be automated.
- Functional characteristics within current DBMS software for implementing Privacy Act compliance actions.

The Privacy Act requirement analysis, provides inputs in the development of a set of data and procedures for compliance with Privacy Act requirements. Those compliance actions identified are slightly different from Goldstein's [7,8], whose compliance actions are used for evaluating a number of alternative compliance methods. For example, revision of forms, training of personnel, etc. are considered in Goldstein's work but are not amenable to implementation in data base management systems.

The second set of data gathered for analysis are the DBMS functional characteristics. A set of data base functions are identified. These data base functions, if incorporated in a DBMS, will in fact realize the Privacy Act compliance procedures.

1.4 Guide to the Reader

The reader is assumed to be familiar with the Privacy Act. Detailed analysis of relevant provisions of the Privacy Act appears in Appendix I. For purpose of this report, the Act's requirements are classified into five functional areas:

- Collection of information
- Maintenance and use of information (by the maintaining agency)
- Data subject access to and amendment of information
- Non-routine-use and disclosures of information, and
- Public notice requirements

These five functional areas are translated into compliance procedures. Supporting these compliance procedures are the data files necessary to perform the compliance actions. Section 3 of this report examines the data base management system functional characteristics in terms of three phases: input, processing, and output. Within each phase, a set of DBMS functions are specified. These DBMS functions are shown in Section 4 to be those which implement specific compliance procedures. The correlation of requirements, compliance procedures, and DBMS functions appears in tabular form in Appendix II. The reference section contains brief annotations.

2. COMPLIANCE: DATA AND PROCEDURES

To develop an implementation strategy for meeting the Privacy Act requirements, it is assumed that an agency has (1) a system of records containing personal information, and (2) a data base management system as nucleus software to process this system of records. The traditional data base environment consists of a data base containing files with records of information, plus a set of supporting application programs.

To accommodate privacy demands, an additional set of application programs and supporting data files are necessary. The design of the data files, and the specification of the application programs which are referred to as compliance procedures, are identified and presented below.

2.1 Data Files and Data Elements

The data needed in support of compliance procedures assumes the existence of a data base containing personal information. This data base is installed on a DBMS which is commercially available. General criteria for data base organization can be quite flexible depending on the data relations of the systems of records being established. Specific files and data elements are suggested here to be incorporated as part of the Privacy implementation data base.

It is also assumed that the data base has an distinct logical segment containing the system of records of individual personal information which will be referred to as the main file. Additional data fields are required for the implementation of Privacy Act compliance procedures. These additional data elements, added to the logical segment, for each data subject record in the main file are:

- Consent field - Yes or No and date of consent.
  - Reference indicating the kind of consent.

- Disclosure Account field -
  - Number of times disclosure to individual himself
  - Number of times disclosure to third-party
  - Number of times special disclosure
  - Number of times disclosure denied
  - Indicator leading to an entry in Disclosure Account (DA) file described later.

Dispute field - Yes or No,
If yes, set indicator leading to Statement of Dispute (SOD) file described later.

Several additional files might be associated with a system of records containing personal information. The specification of these files and the data elements required are identified below. Notice also that the abbreviated file name which appears in parenthesis will be referenced in the compliance procedure tables in appendix II.

STATEMENT OF DISPUTES FILES (SOD). This file contains information of all the disputes. As described above, it is assumed that, in the main file, the individual record containing disputed data about an individual is flagged and a pointer mechanism would lead to a record of this SOD file. Each record would have the following data elements:

- Date of dispute
- Nature of Dispute - Textual description of dispute
- Agency Reason for Refusal - Textual description of refusal
- Status - judicial review or other legal remedies
- Disputed data element name - The data element in dispute
- Disputed data value - The data value in dispute

DISCLOSURE ACCOUNTING FILE (DA). This file contains records of all the disclosures. It is assumed that the individual master records contain three types of disclosure flags: disclosure initiated at the data subject's request, third-party disclosure, and special disclosure. In fact, these flags can be the "count" of each type of disclosure for this particular record. Indices or pointers would lead to the existence of this DA record. Each record in the DA file would have the following data elements:

- Date of disclosure
- Purpose of disclosure - Textual description
- Data elements - List of data element names disclosed
- Data values - List of corresponding values disclosed
- Name - Person or agency to whom disclosure is made
- Address - Person or agency to whom disclosure is made

PUBLIC NOTICE FILE (PN). The law requires that an annual report for each system of records must be submitted by April 30th of each year. The computer maintenance of this file is optional. The PN file may be defined when establishing a new system of records. The contents of the file are used for the announcement notice in the Federal Register and can be maintained also and used for eventual annual review and reporting purposes. The file may contain the following data elements:

- System Name
- System Location
- Categories of Individuals
- Categories of records
- Authority for Maintenance
- Routine uses
- Policies and practices regarding storage
- Policies and practices regarding retrievability
- Policies and practices regarding safeguards

- Policies and practices regarding retention and disposal
- System manager and address
- Notification Procedure
- Record access procedure
- Name and address of administrator for disputing
- Record source categories (how source information is obtained)

NOTIFICATION NOTICE FILE (NN). This may be a small file which can perhaps be a subpart of the PN file. Specific information requirements will be established when the new system of records is in effect. This file may be used to notify individuals of the existence of personal information collection and maintenance by an agency. This file needs to be modified when a new use of an existing file occurs. Data elements consist of:

- The authority
- The purpose
- The routine use
- The effect

STATISTICAL FILE (STAT). The OMB Guidelines [2] require that the agency also keep statistical information. A separate file may be established containing the following data elements such as:

- Number of subjects from whom information is collected
- Number who refuse to provide information
- Number of individuals requesting access
- Number of individuals refused access
- Number of refusals appealed
- Number of cases ending in judicial review
- Number of times time limit was not met by the Agency

2.2 Compliance Procedures

Each Privacy Act requirement identified is translated side-by-side with the compliance procedures using a tabular format. See the first two columns of Appendix II. Within the procedure specification, data file references are made using the acroymn designation indicated in the previous sections.

Five broad areas of Privacy Act requirements are identified to facilitate identification of compliance procedures that are relevant in a DBMS environment. In Appendix II, the compliance procedures for each of these areas are grouped in five separate tables. Table 1 lists the requirements for collection of information. Table 2 lists the requirements for maintenance and use of information by the maintaining agency. Table 3 lists the data subject access, amendment and dispute handling requirements. Table 4 lists the disclosure requirements. The various conditions of disclosures are presented with an additional two columns indicating whether accounting and consent are necessary. Table 5 lists the public notice requirements.

In the next section, relevant DBMS functions will be identified and then related to these compliance procedures.

3. DATA BASE FUNCTIONS

Current data base management functional capabilities are examined to develop a set of technical approaches to privacy compliance procedures. The specifications of the DBMS functions are generic in nature and do not impose any requirements on any particular type of DBMS. These generic DBMS functions identified are specifically relevant for implementing the Privacy Act provisions. These functions are, for purposes of clarity, classified under three functional phases: input, processing, and output. Each function identified under the three phases is numbered and prefaced with the letter "I," "P," and "O" representing input, processing and output phases.

3.1 Input Phase

I1 - Data Collection

Raw data collected from individuals are usually defined to the data base using the data definition facility of the system. Adjunct packages such as a data directory or a dictionary, if available, can be used as a tool to describe each data element to the system. The definition will then facilitate the raw data value collected to be entered into the system.

I2 - Data Entry

The data to be entered into the data base can either be bulk loaded or added into the data base using the update capability. Usually this feature is inherent in the DBMS software.

I3 - Data Validation

The input data need to be validated to insure accuracy and integrity. Techniques range from data type checking to specific semantic consistency checks. Usually some type of data validation feature is inherent in DBMS available today.

I4 - Notification Notice

When establishing new information on a data subject, a notification notice is required by the Privacy Act. This could be an automatic print out of the Notification Notice (NN) file as described in previous section.

I5 - Consent to Disclose

A form letter may be issued to the data subject upon a request to disclose. If consent is given, the "consent" field in the data subject record in the main file is set to "YES." A reference to this "consent" request is recorded. If consent is denied, the "consent" field is set to "NO." At the same time the Statistical File (STAT) field for the number of individuals refused access is incremented by one.

3.2 Processing

P1 - Periodic Validation

The periodic validation for accuracy, relevance, timeliness and completeness is distinguished from data validation upon data input. This requirement is specifically spelled out in the Privacy Act. It is considered good information management practice to allocate certain time and resources for the validation of data integrity. Special software can be written to check the entire data base. The software can utilize the validation routines for data input or can provide a sophisticated checking mechanism specifically tailored for the application.

P2 - Authenticating data accesses

During data retrieval or updating, the user needs to be properly authorized to do the data accesses. Password checking or more sophisticated mechanisms must be provided in the DBMS. However, today's DBMS do provide some method for authenticating the user, and this facility can be considered as inherent in the data base software.

P3 - Retrieval for disclosure

After the user has been authenticated, the nature of disclosure is checked. In Appendix II of this report, the "Conditions of Disclosure" have been identified. Those that required consent of data subject must have the "consent" field checked. Those that required accounting of disclosure must invoke the disclosure accounting procedure (described later - see P6). A retrieval command will produce hard copy output to be given to the requestor. (The Act places restrictions on the use of Social Security number; methodology for retrieving individual records from personal data files using non-unique identifiers are described in [11].)

P4 - Data Update Due to Amendment

The field to be amended is retrieved and the contents of the field are modified as indicated. The disclosure accounting of that record is also retrieved. Names and addresses of individuals are generated. Letters informing them of the correction are then sent.

p5 - Data Purging due to specified record life

Based upon the condition of a specific purging requirement, a set of records that satisfied this condition is retrieved. The identity of records and date of purge are entered into a separate file for backup or audit purposes. These records are later deleted from the data base.

P6 - Disclosure Accounting

Based upon the nature of the disclosure, flags in the data subject record are set in the master file. A record in the Disclosure Accounting file (DA) is created and data values for each data element specified in Section 2 of this report are entered.

P7 - Dispute Accounting

The "Dispute" field in the data subject record in the master file is set. A pointer leading to the record in the Statement of Dispute file (SOD) is created and data values for each data element specified in Section 2 of this report are entered.

3.3 Output

O1 - Publish Annual Notice

Every year, before April 30th, the printout of the Public Notice File (PN) is invoked.

O2 - Publish New Use for Existing System of Records

The data element is modified to reflect the new use in the Public Notice file (PN). The file for the Federal Register announcement is printed out.

O3 - Output Disclosure Accounting

Specific data subject's disclosure accounting record is printed upon request.

O4 - Output Dispute Accounting

Specific data subject's dispute accounting record is printed upon request.

O5 - Statistical output

The Statistic file (STAT) is printed upon request.

3.4 General Implementation Comments

All of the above identified data base functions are easily implementable on any of today's data base systems in the marketplace. Certain functions are available as built-in features of a DBMS. These features can be used as they exist in the software unless more stringent requirements are needed. Other privacy requirements are not directly available in the DBMS and application programs must be written. The following table summarizes the previously outlined data base functions and shows which functions can be implemented by inherent features and which functions require writing of application programs.

Data Base Function	Inherent Feature	Application Program
INPUT		
I1 - Data Collection	X	
I2 - Data Entry	X	
I3 - Data Validation	X	
I4 - Notification Notice		X
I5 - Consent to Disclose		X
PROCESSING		
P1 - Periodic Validation	X	
P2 - Authentication	X	
P3 - Retrieval fot disclosure		X
P4 - Update due to Amendment		X
P5 - Data Purging		X
P6 - Disclosure Accounting		X
P7 - Dispute Accounting		X
OUTPUT		
O1 - Publish Annual Notice		X
O2 - Publish New Use		X
O3 - Output Disclosure Accounting		X
O4 - Output Dispute Accounting		X
O5 - Output Statistics		X

TABLE - DATA BASE FUNCTIONS

The specification of functions is at a generic level where the degree to which the suggested action is implemented is a management decision of the specific agency. For example, software techniques for data validation, or authenticating user access, range from very simple to elaborate but costly algorithms. The amount of validation or security control needed must be decided by each individual agency.

4. DBMS FUNCTIONS TO MEET PRIVACY REQUIREMENTS

The compliance data and procedures as identified in Section 2 can be correlated with the DBMS functions introduced in Section 3. These DBMS functions are implementable either via application programs or inherent in the data base software. Those functions that require the writing of application programs also depend on the existence of the data files described in Section 2 of this report.

In Appendix II, five separate tables are illustrated to cover the five areas of the Privacy Act requirements. These requirements are translated into compliance procedures. The compliance procedures can be realized with the implementation of the DBMS functions indicated.

5. CONCLUSIONS

An implementation strategy for complying with the Privacy Act of 1974 with the use of today's data base management systems is described. A set of DBMS functions, either inherent as built-in data base features, or to be built via application programs, are identified. These functions can be written in the particular DBMS's user language or the host application programming language. These functions, together with the supportive data file specifications, can implement those privacy compliance procedures that are suggested to be automated.

The impact of Privacy Act compliance on the use and design of DBMS are assessed.

5.1 Use of DBMS to comply

Does the use of DBMS significantly improve the capability of meeting Privacy Act requirement? The answer to that question is that the privacy law compliance is not necessarily a justification for employing a generalized data base management system. However, it alleviates certain manual bookeeping activities and therefore provides more consistent journalling by the computer without human errors or omission. Some benefits as well as some negative impacts of the use of a DBMS to achieve compliance are enumerated:

Benefits:

1. The existence of a DBMS will make the implementation of Privacy Act requirements more uniform throughout the data processing user community and substantially simplify the job of administration.

2. DBMS will be able to respond to changing requirements more flexibly and easily. Thus, if new requirements emerge, DBMS will allow certain logical changes without significantly affecting the existing applications.

3. With the increased awareness and emphasis on data base system security procedures and data integrity mechanisms, the inherent capability of DBMS can be used advantageously in support of compliance of the Privacy Act.

4. Usage of application programs written for Privacy Act compliance can be monitored for auditing the administration of the Privacy Act.

5. The use of DBMS facilitates the reporting of statistical and summary data. For example, the reporting of statistics such as the number of disclosures per week or the number of disputes being amended can quickly be accomplished with the use of DBMS.

Negative Aspects:

1. The data base management approach increases the flexibility for interrelating data and for browsing, especially in an on-line access (local or remote) environment. This may facilitate unauthorized use of data. Therefore, adequacy of computer security must be considered.

2. A centrally maintained data base increases the potential consequences of data base destruction, so backup provisions must be made.

5.2 Levels of Automation

Automation in this context refers to privacy compliance activities that are performed by a computer with data base management software. Several possible alternative levels exist:

A. All manual system

B. Data subject records flagged automatically but a paper file is retained.

C. Data subject records flagged automatically with separate automatic journalling of disclosure and dispute accounting.

Level A - The all manual status reflects the majority of Agencies information management practices today. This is partly because the Privacy Act has only been in effect since September 1974 and the agencies are just beginning to develop and design compliance procedures. Also some agencies have not fully converted from second generation data processing techniques to the use of a DBMS, and no software has been implemented.

Level B - This level requires a minimal amount of software effort if the data subject records are already automated with the use of a DBMS. Some agencies require the manual paper file to be kept as evidence of actual written letters for requesting access or disclosure. This is used as proof of authenticity. Therefore, developing software to provide for disclosure accounting and disputing accounting will be an additional effort.

Level C - This is the level where most of the compliance procedures are automated with the exception of issuing letters for acknowledgement purposes. There is no reason why the letters could not also be generated by computer. The functions specified in the report, if properly incorporated in a DBMS, could achieve a high degree of automation. The functions listed also reflect a reasonable level of compliance.

5.3 Problem Areas

The issue of level of compliance is left to the agency's decision. In the areas where the Privacy Act requires a logging activity or issuance of an announcement, compliance is straightforward. However, in the areas of security control and data integrity, just how much is enough is not quantifiable.

A precise definition of minimum level of privacy compliance does not exist. There are also some areas where the law is open to interpretation. For example:

- Keeping track of disclosures to secondary and tertiary users.

- Safeguarding against inferences being made on the data.

- Keeping track of a data subject's consent for a new routine use on an existing system of records.

Such compliance procedures may prove to be prohibitively costly to implement and could unnecessarily over-burden a data base system.

5.4 Summary

The approach of using DBMS to comply with the Privacy Act represents an ad hoc solution using today's systems rather than complete redesign of systems. Privacy Act compliance is not necessarily a justification for employing a DBMS, however, if an agency is using or is contemplating the use of a DBMS, it appears that privacy compliance procedures can be easily incorporated with the data base functions described.

The degree to which the suggested actions are implemented is a management decision of the specific agency. However, the suggested functions reflect an achievable level of compliance.

The administration of compliance can be made easily accountable. In particular, this means the operating cost of Privacy compliance will be easily identifiable via software logging. This factor alone benefited the use of DBMS for Privacy compliance.

The use of DBMS means a more stringent administrative control with the operating environment. The complexity of DBMS environment requires knowledgeable system personnel and data base administrators to control data accesses and systematic logging and reporting. Physical security needs to be tighter to alleviate the fear of potential destruction. Hardware and software need to be "certified" for reliability and quality assurance.

The use of DBMS imposes a more sophisticated requirement for access conttol and data integrity checks in the data base system. Today's DBMS supplied by the vendors have inadequate protection mechanisms for providing controlled accesses. More research in security and integrity techniques is needed in future DBMS to achieve adequate security measures.

REFERENCES

[1] Privacy Act - Public Law 93-579, Dec 31, 1974

The Privacy Act of 1974.

[2] OMB Circular No. A-108, and accompanying "Privacy Act Guidelines," Federal Register Vol. 40, No. 132, July 9, 1975.

This circular defines responsibilities for implementing the Privacy Act of 1974.

[3] National Bureau of Standards, "Index of Automated System Design Requirements as Derived from the OMB Privacy Act implementation Guidelines," NBSIR75-909, Oct. 1975. (Available as PB 246-863 from the National Technical Information Services, Springfield, Va. 22161.)

This index is a list of certain requirements which must be considered by Federal personnel in order to comply with Privacy Act. Each requirement listed contains a reference to an applicable part of the Privacy Act and to a page and column number of the OMB guidelines as they appear in the Federal Register.

[4] Federal Information Processing Standards Publication, FIPS PUB 41, "Computer Security Guidelines for Implementing the Privacy Act of 1974," May 30, 1975. Available From: U.S. Government Printing Office, Washington, D.C. 20402, SD Catalog C 13.52:41.

This document describes technical and procedural means for safeguarding personal data in automated information systems.

[5] Bushkin, Arthur A, & Samuel I. Schaen, " The Privacy Act of 1974: A Reference Manual for Compliance," System Development Corp. 7929 Westpark Dr., McLean, Va. 22101, May 3, 1976.

This document is primarily intended to be a comprehensive reference manual for those people who, in the course of their jobs, must work with information systems subject to the Privacy Act of 1974.

[6] Berg, John (Editor), "Data Base Directions - The Next

Steps" National Bureau of Standards, Special Publication 451, Sept. 1976.

This report is the proceedings of a workshop held in Fort Lauderdale, Florida on October 29, 30 and 31, 1975. Among the five subject areas discussed, the chapter on "Impact of Government Regulation" is particularly relevant for this report. This chapter identifies twenty areas of regulations. The impact of these regulations with a selected set data base system factors is assessed.

[7] Goldstein, Robert C., Henry H. Seward and Richard L. Nolan, "A Methodology for Evaluating Alternative Technical and Information Management Approaches to Privacy Requirements," National Bureau of Standards Technical Note 906, June 1976. Available from: U.S. Government Printing Office, Washington, D.C. 20402, SD Catalog C13,46:906.

This document presents a logical, structured method for evaluating alternative technical and information management approaches for compliance with the Privacy Act. The Privacy Act law is grouped into 4 general requirements. These requirements are translated into compliance steps. Each step contained one or more actions to be taken by the system. If these actions can be accomplished via computer software, then, the algorithm and cost of developing this action is defined. The cost is expressed as parameters to a cost model.

[8] Goldstein, Robert C. and Henry H. Seward, "A Computer Model to Determine Low Cost Techniques to Comply with the Privacy Act of 1974," National Bureau of Standards Interagency Report NBSIR 76-985, Feb. 1976. (Available as PB 250-754 from the National Technical Information Services, Springfield, Va. 22161.)

This document contains a complete description of the steps necessary to run the DPM Cost of Privacy Model along with a description of the computer program.

[9] HEW, "Records, Computers, and the Rights of Citizens," Report of the Secretary's Advisory Committee on Automated Personal Data Systems, DHEW Publication No. (OS)83-97, U.S. Department of Health, Education, and Welfare, July 1973.

This document discusses in detail the rights of citizens as permitted by legislation and recommends actions and responsibilities for the Secretary of HEW.

[10] Office of the Federal Register, National Archives and Records Service, General Services Administration, "Protecting Your Right to Privacy --" No Date.

This document contains a digest of system records of each of the Federal Agencies, Agency Rules of each Agency and research aids.

[11] Moore, G. B. et al., "Accessing Individual Records From Personal Data Files Using Non-Unique Identifiers," National Bureau of Standards Special Publication 500-2, Feb. 1977.

This report describes methodologies for retrieving an individual's record without the use of a universal identifier.

APPENDIX I - PRIVACY ACT REQUIREMENTS

There are a number of ways one can classify the Privacy Act for analysis; the Act itself specifically mentions the "collection, maintenance, use, and dissemination" of personal information, but follows a somewhat different breakdown in the body of the legislation. This breakdown is chosen so that it accords more or less with the flow of information to, from, and within an organization, as such a breakdown appears most useful to the information specialists for whom this report is written. Specifically, the Act will be considered from five viewpoints:

- collection of information,
- maintenance and use of information (by the maintaining agency),
- data subject access to and amendment of information,
- non-routine-use and disclosures of information, and
- public notice requirements.

This section is a brief summary of the requirements of the Act, and should not be used as guidance for general compliance with the Act's provisions. For official guidance, the reader is referred to [2,4]; other guidance may be found in [3,5,7,8]. It is assumed that the reader is reasonably familiar with terms specific to the Privacy Act, such as "system of records," "disclosure," etc. These terms are defined in the Act.

Collection

Clearly, the Act intends that agencies only collect information that is "both relevant and necessary for an agency purpose authorized by statute or executive order" [5]. Furthermore, information collection on the exercise of First Amendment rights is -- with minor exceptions -- specifically prohibited. If information may be subsequently used to make an adverse determination about an individual, then the collecting agency must strive to collect that information directly from the individual himself; if collection from a third party is necessary, then the agency must attempt to verify such information with the individual. When distributing a request for information, the request should be accompanied by an explanation of what the information will be used for, and under what authority it is being collected. All information collected--regardless of source--must be verified by the collecting agency. Reasonable efforts must be demonstrated by the agency to ensure its accuracy and relevance. Furthermore, the information should be noted upon receipt if it is (1) from a third party, and if so, whether verified with the individual or not; (2) obtained with an explicit promise of confidentiality; and (3) sensitive in nature (medical or national security information, for example).

Maintenance and Use

Agencies must maintain and use their personal information records in a manner that ensures fairness to the individuals in question. They must take reasonable precautions against misuse of information, and against use of incorrect or out-of-date information. In particular, they must provide training for employees in the requirements of the Act if those employees will be handling personal information. They must at least annually review information on file to ensure that it is not a record of the exercise of First Amendment rights, and generally to ensure that all aspects of the Privacy Act are continuously being adhered to (this is the "annual review" of the Act). In addition, agencies must purge records after their useful life has expired, but must retain the accounting of disclosures of records (see "Non-routine-use disclosures") for at least five years after the accounting was made, or for the life of the record, whichever is longer. Normally, agencies will only disclose information (1) within the agency, to those employees who have a need to know the information for the regular performance of their duties; or (2) outside the agency, for an established "routine use." Exceptions to these two conditions are discussed under "Non-routine-use disclosures," below. A "routine use" is established through the publication of annual reports and notices: see "Public notice requirements."

Furthermore, agencies must ensure the confidentiality and security of personal records by "establishing appropriate administrative, technical, and physical safeguards" [1] against any anticipated breach of confidence or physical integrity. Agencies would also be wise to consult legal counsel regarding certain issues of records use, such as whether the copying of all or portions of a system of records for internal agency disclosure constitutes itself the creation of a new system of records.

Access, Amendments, and Disputes

The Privacy Act guarantees that an individual be able to determine the existence of any information about him in any agency's system of records, and that he be able to see, have a copy of, and correct such records. Thus agencies are called upon to establish procedures to provide these four guarantees. When disclosing information to a requesting individual, however, the agency can filter the information to remove: (1) items having possible adverse effects on the individual (medical information, for example);

(2) confidential sources of information (if an implied promise of confidentiality was given to the source before Sept 1974; or an explicit promise after that); (3) CIA or criminal law enforcement information; (4) classified national defense information; (5) information about protection of the President of the U.S.; (6) information required by statute to be for statistical purposes only; (7) investigatory material compiled for employment checks; (8) testing and examination material for employment; and (9) information regarding future promotions (in the military).

Each access by an individual to his own records is to be considered a disclosure by the maintaining agency, and as such, must be logged in the agency's accounting of disclosures (see "Non-routine-use disclosures"). In addition, if the individual so requests, the agency must provide access to that accounting of disclosures, so that an individual may determine what information about him is being disseminated, to whom, and for what purpose. The agency may not require that the requesting individual know particular identifying codes or numbers unique to the system of records in question in order to facilitate the agency's finding relevant information; it must be sufficient that he know such common particulars as name, age, place of birth, residence, etc. The information so disclosed must be in a form comprehensible to the requesting individual, and the individual may, if he wishes, be accompanied by a person of his own choosing.

Of pivotal importance to the letter and spirit of the Act is the requirement that an individual be allowed to correct erroneous information about himself. Thus agencies must establish procedures to permit individuals to submit corrections to their records. If the agency acknowledges an individual's correction, it must make the correction and inform all previous recipients of the erroneous information of its corrected content. Should the agency determine, however, that a correction is unwarranted, it must permit the individual to file a statement of dispute. A notation of that statement must be made integral to the record in question, and the dispute statement itself must be included with subsequent disseminations of the record. The agency may also file its own reasons for denying the correction, and disseminate those reasons along with the record and associated dispute statement.

Non-Routine-Use Disclosures

If disclosure of information is not within the agency, not for a published routine use, and not to the individual subject of the records, then in general the agency must obtain permission from the subject to make the disclosure. Even with that permission, however, disclosure is at the agency's discretion. Exceptions to this requirement for permission occur in cases of disclosure to the following (parentheses indicate whether disclosure is at the agency's discretion):

- to Congress (discretionary)
- for law enforcement (discretionary, unless overridden by statute)
- under compulsory legal process (not discretionary)
- in an emergency (discretionary)
- for statistical purposes (discretionary)
- to the Census, GAO, or National Archives (discretionary, treated essentially the same as a routine use disclosure)

If disclosed to other than another goverment agency, information must be verified for accuracy, relevance, timeliness, and completeness and filtered to remove information not relevant to the request. If a statement of dispute is relevant to the disclosure, that statement must of course be included. An accounting of the disclosure must be made. Information disclosure may be requested under the Freedom of Information Act, and if that Act is relevant, disclosure may not be denied, nor need an accounting be kept.

Public Notice Requirements

A fundamental provision of the Privacy Act that echoes the HEW Report [9] is that no system of records can be secret in its very existence. To this end, the Act requires extensive public announcements concerning each agency's system of records, and certain announcements to the Congress.

Public notice must be given (in the Federal Register) (1) of any new system of records; (2) of any new routine uses for existing systems of records; and (3) annually for all systems of records. A significant change, say in the number, type or categories of individuals in the system, or the potential for access to existing records, can trigger the requirement for a new system of records notice. Furthermore, agencies must report to Congress on their activities under the Privacy Act. Specifically, they must provide a report (1) on any proposed new system of records, and (2) annually on all systems of records and on a number of facets of compliance with the Act, e.g., information system plans, improvements in records management policies and procedures, problems with compliance, statistics on the number of inquiries, amendment requests, denials of requests, and so on.

APPENDIX II - CORRELATIONS OF REQUIREMENTS/COMPLIANCE PROCEDURES/DBMS FUNCTIONS

TABLE 1 - DATA COLLECTION REQUIREMENTS

DATA COLLECTION REQUIREMENTS	COMPLIANCE PROCEDURES	DBMS FUNCTIONS
1. Collect information from individual	. Design data entry form together with notification notice	I2
2. Inform individual of Privacy Act statement	. Issue notification notice	I4
3. Limit collection of information on exercise of first amendment rights		
4. Be able to function without Social Security Number		

TABLE 2 - MAINTENANCE AND USE REQUIREMENTS

MAINTENANCE AND USE REQUIREMENTS	COMPLIANCE PROCEDURES	DBMS FUNCTIONS
1. Maintain data accuracy, relevance, timeliness, and completeness	. Periodic verification of data	P1
2. Purge records after their useful life has expired - disclosure accounting five years later	. Software to delete records based on criteria	P5
3. Make an accounting of the purge	. Log the date purged and what is purged	P5

TABLE 3 - ACCESS, AMEND, AND DISPUTE REQUIREMENTS

REQUIREMENTS	COMPLIANCE PROCEDURES	DBMS FUNCTIONS
ACCESS		
1. Inform individual whether a system of records contains a record pertaining to him upon request	. Notification to subject	I4
2. Permit individual to review records pertaining to him	. Verify identification of ind. . Retrieve the record via software	P2 P3
3. Permit individual to be accompanied		
4. Permit the individual to obtain a copy of such record	. Print out specified contents of data elements	P3
AMENDMENT		
1. Amendment request originates from individual		
2. Agency send written acknowledgement of the receipt of the amendment request within 10 days	. Issue form letter acknowledging receipt of amendment request	
3. Agency agrees to amend		
3a. Advise individual	. Issue form letter informing of the acceptance	
3b. Correct the record	. Modify the record via software	P4
3c. Advise all previous recipients of the correction	. Retrieve disclosure accounting for that record . Issue letter informing of the correction and substance of the correction	O3
4. Agency refuses to amend		
4a. Inform individual of its refusal (reasons and name-address of official for further review)	. Issue form letter of refusal	
DISPUTE HANDLING		
1. Individual files with the agency a statement of dispute	. Mark the 'dispute' bit in the record . Create a dispute record. See data element for SOD file	P7 P7
2. Provide prior recepients with a copy of dispute statement	. Print out the disputed record and mail to previous disclosure recipients	O4

TABLE 4 - DISCLOSURE REQUIREMENTS

CONDITIONS OF DISCLOSURE	ACC. REQ.	CONS REQ.	COMPLIANCE PROCEDURE	DBMS FUNCTIONS
ROUTINE USE				
Interagency transfer of records for the purpose for which it was collected	N	N		
NORMAL USE				
Intra-agency employers who have need for the record in the performance of their duties.	N	N		
SUBJECT				
Access by data subject	Y	N.A.	(See ACCESS section)	P2
FREEDOM OF INF. ACT				
Disclose records to the public under the Freedom of Information Act	N	N		P3
THIRD PARTY				
Disclose to third party	Y	Y	. Generate letter to obtain consent . Set 'consent' field to be Y/N . If yes, software to retrieve claimed information and enter disclosure accounting. For data element see DA file . If no, notify person requesting data that consent was denied. Log denied disclosure accounting	 I5 P3 P3

TABLE 4 - DISCLOSURE REQUIREMENTS (CONT'D)

SPECIAL DISCLOSURES			. Set special disclosure bit	P3
1. To the Bureau of Census	Y	N		
2. For Statistical research and reporting	Y	N	. Remove personnel identifier	05
3. To national archives	Y	N		
4. To law enforcement purpose at the written request of an agency head	Y	N		
5. Under emergency circumstances affecting an individual's health and safety	Y	N	. Subsequent notification to ind.	
6. To the Congress	Y	N		
7. To the General Accounting Office	Y	N		
8. Pursuant to a court order	Y	N		
RETROACTIVE DISCLOSURE				
1. Access by data subject for disclosure accounting	Y	N.A.	. Print disclosure accounting record, but not the special disclosures	03
2. Request for disclosure accounting by other indiv	Y	Y	. See THIRD PARTY section	
3. Inform past recipients of disputed or corrected inf	Y	N.A.	. See DISPUTE HANDLING	

TABLE 5 - PUBLIC NOTICE REQUIREMENTS

PUBLIC NOTICE REQUIREMENTS	COMPLIANCE PROCEDURE	DBMS FUNCTIONS
ANNUAL REPORT		
Annual notice of Agency rule and record system descriptions	. Record system description and Agency rule may be stored and printed out via computer. (Data element - See Public Notice file.)	01
ANNUAL REVIEW		
Is all information relevant, necessary, timely and complete?	. Develop software to support audit compliance program	P1
Is agency's record keeping practices consistent with the Act		
NEW SYSTEMS NOTICE		
Publish in Federal Register at least 60 days ahead of use	. Print out public notice file	01
NEW USE NOTICE		
Publish in Federal Register a new use report 30 days ahead	. New use notification to data subject . Modify NN file	02 02

NBS-114A (REV. 7-73)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET	1. PUBLICATION OR REPORT NO. NBS SP-500-10	2. Gov't Accession No.	3. Recipient's Accession No.

4. TITLE AND SUBTITLE

COMPUTER SCIENCE & TECHNOLOGY:

A Data Base Management Approach to Privacy Act Compliance

5. Publication Date

June 1977

6. Performing Organization Code

640.02

7. AUTHOR(S)

Elizabeth Fong

8. Performing Organ. Report No.

9. PERFORMING ORGANIZATION NAME AND ADDRESS

NATIONAL BUREAU OF STANDARDS
DEPARTMENT OF COMMERCE
WASHINGTON, D.C. 20234

10. Project/Task/Work Unit No.

640.1221

11. Contract/Grant No.

12. Sponsoring Organization Name and Complete Address (*Street, City, State, ZIP*)

Same as Item 9

13. Type of Report & Period Covered

14. Sponsoring Agency Code

15. SUPPLEMENTARY NOTES

Library of Congress Catalog Card Number: 77-608106

16. ABSTRACT (*A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.*)

The Privacy Act (PL 93-579) provisions on personal record handling present new issues concerning effective use of commercial data base management systems (DBMS) by Federal agencies. The widespread use of such systems in recordkeeping activities will definitely have an impact on methods of administering compliance with the Privacy Act. This report proposes a technical approach to compliance with certain Privacy Act requirements through the use of generalized data base management system. Requirements are translated into a set of computer data file and procedures. These procedures, incorporated at pivotal points of data base software, can implement those Privacy Act compliance procedures amenable to automation. The use of DBMS appears to be a viable and technologically feasible solution to the effective and efficient implementation of many Privacy Act provisions.

17. KEY WORDS (*six to twelve entries; alphabetical order; capitalize only the first letter of the first key word unless a proper name; separated by semicolons*)

Computer utilization; data base functions; data base management systems; Privacy Act of 1974; privacy compliance techniques.

18. AVAILABILITY ☒ Unlimited

□ For Official Distribution. Do Not Release to NTIS

☒ Order From Sup. of Doc., U.S. Government Printing Office
Washington, D.C. 20402, SD Cat. No. C13.10:500-10

□ Order From National Technical Information Service (NTIS)
Springfield, Virginia 22151

19. SECURITY CLASS (THIS REPORT) UNCLASSIFIED	21. NO. OF PAGES 34
20. SECURITY CLASS (THIS PAGE) UNCLASSIFIED	22. Price

USCOMM-DC 29042-P74

☆ U. S. GOVERNMENT PRINTING OFFICE : 1977--240-848/182

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SCIENCE & TECHNOLOGY

Superintendent of Documents,
Government Printing Office,
Washington, D. C. 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Bureau of Standards Special Publication 500-.

Name ____

Company ____

Address ____

City ____________________ State ______________ Zip Code __________

(Notification key N-503)