U.S. DEPARTMENT OF COMMERCE
National Technical Information Service

PB-259 714

Implications of Privacy Legislation on the Use of Computer Technology in Business

National Bureau of Standards, Washington, D C

1976

NBS-114A (REV. 7-73)

322061

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET	1. PUBLICATION OR REPORT NO. See Item 15	2. Gov't Accession No.	PB 259 714

4. TITLE AND SUBTITLE

IMPLICATIONS OF PRIVACY LEGISLATION ON THE USE OF COMPUTER TECHNOLOGY IN BUSINESS

5. Publication Date Fall 1976

6. Performing Organization Code

7. AUTHOR(S) *RUTH M. DAVIS*

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.

11. Contract/Grant No.

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

Same

13. Type of Report & Period Covered Final

14. Sponsoring Agency Code

15. SUPPLEMENTARY NOTES Jurimetrics J. 17, No. 1, 95-110 (Fall 1976)

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 National Bureau of Standards has been charged with responsibility for developing guidelines and standards for government compliance with legislation to protect individual privacy. NBS has identified emerging problems in security and privacy and the need for technological developments to provide solutions. Safeguards for security and privacy are not identical. The large number of record systems processing personal records in both the public and private sectors points up the magnitude of the problem of retrofitting these systems for security and privacy safeguards. In many cases, sophisticated systems are not required, and good information practices will be sufficient to meet the requirements. The safeguards differ for each system. There is also a need for auditing techniques to check on the effectiveness of the safeguards put into place. The techniques developed will be useful in preventing computer fraud, assuring functional fidelity and maintaining data integrity during input and processing.

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 security; information handling; privacy; safeguards for security and privacy; technology for security and privacy

18. AVAILABILITY [xx] 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

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

19. SECURITY CLASS (THIS REPORT) UNCLASSIFIED

21. NO. OF PAGES

20. SECURITY CLASS (THIS PAGE) UNCLASSIFIED

IMPLICATIONS OF PRIVACY LEGISLATION ON THE USE OF COMPUTER TECHNOLOGY IN BUSINESS*

Ruth M. Davis†

INTRODUCTION

Legislation has already been enacted imposing requirements in Federal government agencies to protect individual privacy. Legislation has been proposed for the private sector which could impose similar requirements and, thereby, change some of the basic thinking of businesses regarding the uses of computers. Increasing emphasis will be placed on requirements reflecting the rights and interests of the individual, the organiza-

*This paper was presented on May 14, 1976 to the American Bar Association Section of Science and Technology First National Institute held in New York City. It was presented by Robert Blanc, who is a member of Dr. Davis' Staff. This paper has been approved by the National Bureau of Standards for publication in *Jurimetrics Journal*.

†Ruth M. Davis is Director of the Institute for Computer Sciences and Technology of the National Bureau of Standards, United States Department of Commerce, Washington, D.C. 20234.

tion, or society. This emphasis will in turn lead to requirements for new or added safeguards and procedures in computer system operation and usage.

At the National Bureau of Standards, we've been concerned with related problems since 1972. That's when our computer security program was initiated under our Brooks Act mandate to provide standards and technical advisory services for government-wide usage to increase the effectiveness of computer utilization. Our privacy effort is subsumed under our security effort. Following the signing by President Ford of the Privacy Act on December 31, 1974, the Office of Management and Budget, under authority assigned to it by the Act, directed NBS to issue standards and guidelines on computer and data security. These were intended to prescribe technical safeguards to insure government-wide compliance with the Privacy Act. Since our program was established in 1972, we have continuously interacted with government and private sector groups to assess the emerging problems surrounding these issues--security and privacy--in establishing directions for our technological program. I would like to share with you some of our findings, particularly those that provide a portent of the impact of privacy legislation on the use of computers in business. Specifically, I'll discuss the public concern over privacy and information abuses, how these have been translated into legislation, and the impact of that legislation in terms of the required technological responses. These requirements should be indicative of anticipated changes in practices concerning computer usage.

PUBLIC AND GOVERNMENT CONCERNS WITH INFORMATION MISUSE

Let me first discuss the concerns and then turn to the technology. Recordkeeping, along with information handling, is a key service industry today and is a most important activity of any large organization—either private business or public. As such information activities increase misuse of information and failures in recordkeeping have become more common and of much greater public concern. Most large information systems activities in business are now automated or computerized. Information abuses and recordkeeping failures are thus abuses and failures of automation and computer systems. As might be expected, eliminating or reducing problems with information has become synonymous with resolving problems associated with the utilization of computer systems for information handling whether concerned with the public or private sectors.

Public concerns with information misuse have manifested themselves in the last five years primarily as concerns over:

- invasions of individual privacy,
- centralization of information control, e.g., as with the FBI and State/local governmental controls over criminal records,
- damage to individuals resulting from inaccuracies in credit records,

- controlling unlawful access to and unlawful use of "valuable" information, as for example, in electronic funds transfer, agricultural commodity listings and health records, and
- computer fraud.

SECURITY V. PRIVACY

Almost all problems of information misuse and failures in recordkeeping by automated or computer systems are heavily dependent for their solution upon computer automation, information, and/or communications technology. These problems have become commonly grouped into two major areas: namely; computer security and individual privacy. Computer security and privacy are not identical. Likewise, security safeguards and procedures are not identical with privacy safeguards and procedures.

Computer security addresses problems common to all computer systems. Computer security insures that:

- only authorized information enters the system,
- only authorized users have access to systems,
- only authorized programs are run on systems,
- only authorized changes are made to programs,
- only authorized individuals access outputs, and
- there is no destruction of the facilities, information or programs.

On the other hand, privacy is concerned only with information on individuals and, therefore, addresses only a subset of computers. As detailed in the Privacy Act, privacy means:

- that there will be no secret data bases,
- that data subjects have a right to access data,
- that data subjects have a right to correct data,
- that data subjects have a right to control dissemination of data, and
- that recordkeepers are responsible for required information controls and notification of data subjects.

RETROFITTING COMPUTER SYSTEMS TO MEET PRIVACY REQUIREMENTS

The Privacy Act was signed into law in 1974. This law became effective some twenty years after the use of electronic and digital computers had become a principal means for information handling in the United States. Prior to the 1970s, based on both customer demands and industry goals, computer systems had been designed principally to meet the objectives of high equipment reliability, increasing speeds of operation, increased efficiency of system operation, and strict requirements for precision. Today, based on heightened awareness of the problems accompanying unanticipated effects of technological change, we are in-

volved with retrofitting existing computer systems designed against specific requirements to meet additional new objectives exemplified by the Privacy Act. The magnitude of the retrofitting dimension of the privacy problem can be examined by first looking at the inventory of computer systems in the government and the private sector.

Federal Government

The General Services Administration inventory of ADP equipment (September 1974) and federal agency published inventories of "personal files" (Federal Registers of 1975) show that sixteen agencies account for 90 percent of the federal computer inventory. The sixteen agencies are AID, DOC, CSC, DOD, DOJ, DOT, FPC, HEW, HUD, NASA, NSF, SCC, TVA, Treasury, USIA, and VA. These sixteen agencies account for approximately 69 percent of the reported 6,700 systems of records and 89 percent of the federal computer inventory. Thus, most of the automated systems of records are included in this sample. By extrapolation from the ratio of general management category systems to automated systems of records, it can be inferred that, as of January 31, 1976, some 1,343 automated systems of records exist in the federal government.

It is difficult to estimate the number of computer systems which process the estimated 1,343 automated systems of records. Based on experience, we can assume that 15 percent of the computers in DOD process personal data and 50 percent of all other federal government do so. Then there are about 715 computers in the federal inventory which process personal data. This then gives an estimate of the magnitude of the computer system retrofit problem in the federal government.

State Governments

In state governments, NASIS has identified 496 computers in the agencies of forty-nine states reporting in 1974 (this excludes higher education, a category dropped for the 1974–1975 report). Since state agencies are not engaged in extensive scientific research or military work and since computers may be shared among many applications, perhaps 70 percent of these computers or about 350 process some type of personal information.

Private Sector

Many information systems containing information about individuals are maintained by organizations in the private sector. Often the information produced by these systems is the product or service supplied in the market-place by the organization. In other cases, the business of the organization is dependent upon the operation of their computerized individual recordkeeping systems.

One basis for priority to retrofit is in terms of public concern. In

February of 1973 we convened at NBS in conjunction with the Association for Computing Machinery a task force on computers and privacy. The findings of that task force, coupled with other activities in which NBS has been involved, allows us to identify eleven major special interest communities in the private sector or public service sector whose record-keeping activities were of greatest public concern. Of greatest concern to the public in terms of privacy problems were:

- public and private schools and colleges,
- criminal and justice law enforcement, and
- commercial credit reporting.

Of lesser concern to the public in terms of privacy problems were;

- banking and finance,
- welfare,
- health care,
- social research,
- insurance,
- statistical studies,
- mail order list companies, and
- personnel and employment reporting.

The priority for retrofitting existing computer systems to meet the requirements of the laws can presumably be established in terms of this or other less subjective measures of public concern. One approach is to estimate effected computer systems by aggregating CPUs installed by S.I.C. (Standard Industrial Classification) Codes considering only those areas most likely to process personal data. Routine payroll and personnel applications, while candidates, are not included. Education, including state education, is included. The number of CPUs installed and the fraction estimated to be processing personal data in these major categories are as follows:

Area	CPUs (Total)	CPUs Fraction Processing Personal	Number Processing Personal
Finance	7085	76%	5400
Non-professional services	7980	12%	950
Professional services	9635	61%	5900
Total	24700	50%	12250

The fractions were determined by estimating the weighted averages for each subcategory. For instance, it was estimated that of the 3,095 CPUs used in banking 80 percent or 2,476 CPUs had some processing function which involve personal data. While it is clear that these conclusions are only approximate, it is equally clear that they establish a reasonable level of installed CPUs which process at least some personal data.

Thus, for the areas considered 12,250 CPUs are involved in the processing of personal data.

RELEVANT REQUIREMENTS OF PRIVACY LEGISLATION

In considering the requirements which may be placed upon the business community due to potential privacy legislation, it is useful to consider the parallel situation in government. Using the Privacy Act as a model numerous requirements are imposed upon Federal agencies to prevent the misuse of data about individuals, respect data confidentiality, and preserve data integrity. The major provisions of the Act which most directly involve computer functions and technical solutions are:

- limiting disclosure of personal information to authorized persons and agencies,
- the requirement of accuracy, relevance, timeliness, and completeness of records, and
- the requirement of the use of safeguards to insure the confidentiality and security of records.

Although the Act sets up legislative prohibitions against abuses technical related procedural safeguards are required in order to establish a reasonable confidence that compliance is indeed achieved. It is thus necessary to provide a reasonable degree of protection against unauthorized disclosure, destruction or modification of personal data, whether intentionally caused or resulting from an accident or carelessness.

Technical Safeguards Required

Let me categorize the kinds of safeguards that are necessary to provide this protection. The categories include:

- physical security measures—measures for protecting the physical assets of a system and related facilities against environmental hazards or deliberate actions.
- information management practices—procedures for collecting, validating, processing, controlling, and distributing data.
- computer system security controls—techniques available in hardware and software of a computer system or network for controlling the processing of the access to data and other assets.

The relevance and utility of technical safeguards can be grasped quickly if they are viewed in the context of the Privacy Act of 1974. Figure 1 identifies the principal provisions of the Privacy Act which involve the application of safeguards and shows how each of the three categories can contribute to the implementation of these provisions. The matrix also serves to illustrate graphically that adopting particular safeguards may help to satisfy more than one requirement of the Act. Significantly, it also indicates that protection of data in automated systems is

not necessarily dependent upon complex computer systems network technology, but can be achieved in good measure by the prudent use of physical security measures and information management practices.

Technical Safeguards v. Control Points

In addition to viewing technological safeguards in terms of the provisions of enacted or potential privacy legislation, it is useful also to view them in terms of the control points within a computer system or network where security risks occur and where appropriate safeguards can be applied. This perspective is provided in Figure 2 which portrays the elements of a computer system/network, progressing through the many possible processing modes, including the use of interacting terminals at local and remote locations and the linking of local systems via communications networks. It stresses again the value of physical security and information management practices as major adjuncts to the computer system/network security controls.

Technical Safeguards v. Computer System Characteristics

Not all computer systems will require exactly the same safeguards. For example, the technical safeguards that are needed to insure privacy differ greatly with respect to the size of the computer system involved. For example, if a system of records is kept on a small isolated minicomputer, then the techniques needed to meet privacy requirements are not much different from those needed for a manual system of records kept in a file drawer. In the case of the minicomputer, as well as for the file drawer, access to the system of records can be controlled manually and other privacy requirements can generally be met by manual techniques. If that system of records is transferred to a large computer or if the minicomputer is connected to a larger computer network, then the information in the file is potentially more widely accessible. A major motivation for privacy legislation stems from the potential for using computers to asssemble information from different systems of records and to use it for purposes other than that which was originally intended.

The extent to which computer systems must be retrofitted with specific technical safeguards varies not only with the size of the computer system but also with all of the following characteristics of the system:

- the type of processing done on the system; e.g., a time-sharing system has different requirements from a batch system and one that allows user programming is different from one that only supports queries or information retrievals.
- the sensitivity and potential value of the personal information determine the potential threat or hazards to the information that can reasonably be expected.
- the security and privacy controls that are already in place, deter-

mine how many additional technical safeguards must be added to meet privacy requirements.

Unfortunately, there is little detailed data available about how much sensitive personal information is processed on what type of computer systems and about the extent of privacy and security controls that may already be incorporated in the systems. The cost of retrofitting computer systems to meet privacy requirements, however, may not be as great as has generally been expected. A principal reason is that privacy requirements are only one of the additional requirements being levied in an over-all effort to implement better information management practices in data processing facilities. For example, much of the technology needed for privacy is also needed for:

- prevention of computer-related fraud,
- accuracy and integrity of data handled by computer systems, and
- effective accountability, auditability, and fidelity of computer systems.

As an illustration, identification and authentication of system users is needed for all these reasons, as well as to meet privacy requirements.

THE TECHNOLOGY OF PRIVACY RELATIVE TO GOOD INFORMATION MANAGEMENT PRACTICES

I have been referencing the "technology needed for privacy." Let me point out that neither security nor privacy has been the object of any technology until recently. "Security technology" is now somewhat developed. "Privacy technology" except when identical with aspects of security technology really does not exist in any organized way. Let me, therefore, discuss the technology of privacy relative to good information management practices.

Information management is just one component of the management process. To try to make it inseparable from management in its entirety is to hinder progress in both information management and the generalized process of management. To illustrate the extent of information management: it begins once the step is completed of deciding what information is desired for the management process in question. It does not include the use of the information by managers or the actions taken as a result of the information presented.

Information management does include management of the activities of:

- data collection,
- data validation,
- data transformation,
- recordkeeping, information manipulation, and storage,
- information controls (including the operations associated with freedom of information and confidentiality of information),
- system accountability, auditability, and fidelity,

- information dissemination and presentation, and
- standardization for information management.

The adequate performance of information management as thus described is an integral and essential part of the entire management process.

The requirements of privacy legislation (enacted and potential) viewed technically generally fall within the information management activities of:

- data collection,
- recordkeeping, information manipulation, and storage,
- information controls,
- system accountability, auditability, and fidelity, and
- information dissemination and presentation.

Within these five areas of information management activity, the major provisions of privacy legislation (using the Privacy Act as a model) which most directly involve computer system/network management practices are:

- the limiting of disclosure of personal information to authorized persons,
- the requirement of the maintenance of accurate, relevant, timely, and complete records, and
- the requirement of the use of safeguards to insure the security and integrity of records.

In addition, although the Act sets up legislative prohibitions against unauthorized disclosures, system/network controls are also needed to help assure that access to personal data is properly controlled and that intentional or accidental violations of security and integrity do not occur. These latter type controls will be considered to be more related to security oriented practices than privacy oriented practices.

NBS has developed in its "Computer Security Guidelines for Implementing the Privacy Act of 1974" (FIPS PUB 41, May 30, 1975), a set of privacy-oriented information management practices recommended for Federal agencies. They are presented as guidelines under the topics of:

- handling of personal data,
- maintenance of records to trace the disposition of personal data,
- data processing practices,
- programming practices,
- assignment of responsibilities, and
- procedural auditing.

Auditing in Privacy Accounting

The most recent literature of EDP auditing shows the procedures that a financial auditor should take are to a great extent independent of the fact that it is a financial system that is undergoing audit. The auditor

is not primarily looking for a good audit trail, but rather for good internal controls. Types of internal controls are:

- organization control,
- hardware control,
- software control,
- program control,
- output control, and
- system control.

Using descriptions of these controls from auditing literature, it is clear that they could just as easily be applied to personnel records as to inventory and accounts receivable.

Current methods of auditing data systems cannot be said to be formalized even though they may represent the best practice available. The state-of-the-art at present does not permit a formalization. The problem of assuring accountability and fidelity is made very difficult by the following fact: for any computer system that has software as a component, no claim of system accuracy can be guaranteed. There is no way to theoretically prove, using the techniques of logic and mathematics, that software actually performs its intended function in all cases and over all conditions.

NBS has inaugurated a research program leading to the eventual development of guidelines for software auditability. Research is required using a statistical and engineering approach because of the lack of available mathematical theory of a deterministic nature. Areas of investigation include:

- program design concepts which reduce the number of total combinations of conditions needed to be examined and other concepts which concern final organization and manipulation,
- program testing concepts including the adding of trace routines which examine the paths taken in program execution, and other concepts which involve testing programs against a variety of input parameter conditions, and
- zero defect data entry involving methods of assuring the correctness of input data.

The work of NBS is aimed at formalized techniques of data systems auditing and may help establish the body of knowledge which a professional auditor would use to audit a personal data system.

SPECIFIC TECHNICAL IMPLICATIONS TO THE BUSINESS COMMUNITY OF PRIVACY REQUIREMENTS

I have discussed privacy legislation requirements in terms of technical safeguards and information management practices. I want to now identify specific requirements in terms of their impact on computer usage.

[illegible] privacy legislation [illegible] technical implications stem from the following requirements:

- data disclosure,
- disclosure accounting,
- right to access and review,
- data protection, and
- data use.

Regulations regarding *data disclosure* require that agencies must obtain written consent from each data subject for the disclosure of personal data other than for routine uses. Prior to the disclosure of personal data the agency must, therefore, check to determine that the requested disclosure is legitimate. Furthermore, if the data subject has previously both given permission for a disclosure of personal data and filed a dissenting claim concerning the data held on him, then the dissenting claim must be forwarded to the person or agency requesting the data.

Disclosure accounting requires that each agency maintain a list of organizations that have regular access to the personal information and employees that have regular access. A separate usage log of nonregular accesses must be maintained. Procedures in software must be developed to maintain this usage log as disclosures are made recording all such disclosures. Purging facilities should also be considered.

The *right to access* and review requires each agency to allow an individual to inspect all data held on him and to access the usage logs of the information about him. Furthermore, an organization must investigate all complaints concerning possible inaccuracies in data held on an individual and if agreement cannot be reached must attach a statement of dispute to each record. That dissenting claim must then be forwarded to any person or agency requesting the data. The claim must be retroactively disseminated to all persons or agencies to whom the data was previously disclosed.

Data protection requires the establishment of the appropriate safeguards as I have already discussed to protect personal information. *Data use* requires that the information be appropriate, relevant as well as accurate, complete, and timely.

These five requirements have the greatest technological impact. In addition, the Privacy Act prohibits the use of the Social Security Number as an identifier unless authorized by law. This means that other techniques must be developed to uniquely identify individuals with records stored on computer systems. NBS is completing the development of guidelines on the use of non-unique identifiers in combination to uniquely identify individuals consistent with the specific needs of an organization.

TECHNOLOGICAL COSTS OF PRIVACY AND GOOD INFORMATION MANAGEMENT

I want to now briefly address the issue of the technological cost of privacy requirements to an organization. There should be high priority

on estimates of the technological costs of privacy. The reasons are several, for example:

- selecting from alternative approaches to problem resolution depends upon knowing associated costs,
- determinations of the pace demanded of government and business in making changes in their information management practices and the date set for implementing required practices depends upon costs to users, vendors and customers, and
- technological costs of privacy should be viewed in the bigger context of benefits ascribable to other areas of good information management practices.

Using the Privacy Act of 1974 as a model and in looking at the technological costs of privacy, the relevant sections of the Act are:

- "Collect information to the extent practical directly from the subject individual . . .";
- "Maintain all records which are used . . . in making any determinations about an individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary . . .";
- "Prior to disseminating any record about an individual to any person or another agency . . . make reasonable efforts to assure that such records are accurate, complete, timely, and relevant . . .";
- "Maintain . . . only such information about an individual as is relevant and necessary to accomplish a purpose . . . required to be accomplished . . .".

NBS has been engaged in and is sponsoring projects aimed at determining the technological costs to Federal agencies of meeting the requirements of the Privacy Act of 1974; the work is based upon the use of one selected computerized model. The determination should also prove useful to the business community anticipating privacy controls. Since the model does not specifically address recordkeeping costs *per se*, representative costs cannot be broken out for all recordkeeping activities. Specific recordkeeping activities which are costed out are:

- collecting data directly from the subject,
- maintaining accurate and complete records, and
- eliminating all but necessary data, for example, purging.

This model, which was adapted to the Privacy Act of 1974 by D.P. Management Corporation under contract to NBS, is currently available through NBS.

CONCLUDING COMMENTS

I would like to conclude by highlighting six points from my presentation:

1. Security safeguards and privacy safeguards are not identical. Technologically, security safeguards subsume privacy safeguards.
2. The problem of meeting the requirements of legislation for technical safeguards is exaggerated because systems do not have designed-in safeguards and obviously cannot all be replaced by new systems. It is, therefore, necessary to retrofit safeguards and this retrofitting is more costly.
3. Sophisticated security safeguards are not necessary in all cases. A fundamental technological basis for security and privacy includes the proper application of good information management practices, which for some installations, will be sufficient to meet requirements.
4. Consistent with 3, above, not all computer systems require the same safeguards. Technical safeguards needed are highly system dependent and determinations must include risk analysis. Each organization must ultimately be responsible for the appropriate selection of safeguards to meet requirements as well as for the consequences of incorrect decisions.
5. Auditing techniques for computer systems need to be developed to check the security of systems during actual operation. This problem is subsumed by the general one of developing auditing techniques and diagnostics to verify, in real-time, that computer systems are performing their intended functions accurately and are not performing non-intended functions. This can be called the *functional fidelity* of computer systems. Finally,
6. Privacy requirements are only one of the additional requirements being levied in an overall effort to implement better information management practices in data processing facilities. Much of the technology needed for privacy is also needed for prevention of computer fraud, for assurances of functional fidelity, and for maintaining data integrity during input and processing.

SAFEGUARDS	REQUIREMENTS: Control of Disclosures	Accounting of Disclosures	Provide Access to Records	Inclusion of Disputed Information	Use Relevant Data Only for Authorized Purposes	Maintain Accurate, Complete Records	Insure Integrity, Security and Confidentiality of Records	Retention of Records; Archival Storage
Physical Security								
Entry Controls	x						x	
Storage Protection	x					x	x	x
Information Management Practices								
Data Processing Practices	x	x		x	x	x	x	
Programming Practices	x	x		x	x	x	x	
Assignment of Responsibilities	x						x	x
Procedural Auditing	x	x		x		x	x	x
Systems Security								
Identification	x		x		x		x	
Access Controls	x		x		x	x	x	
Access Auditing	x	x	x		x		x	x
Data Encryption	x				x	x	x	x

Technical Safeguards Applied to Requirements of the Privacy Act of 1974

FIGURE 1

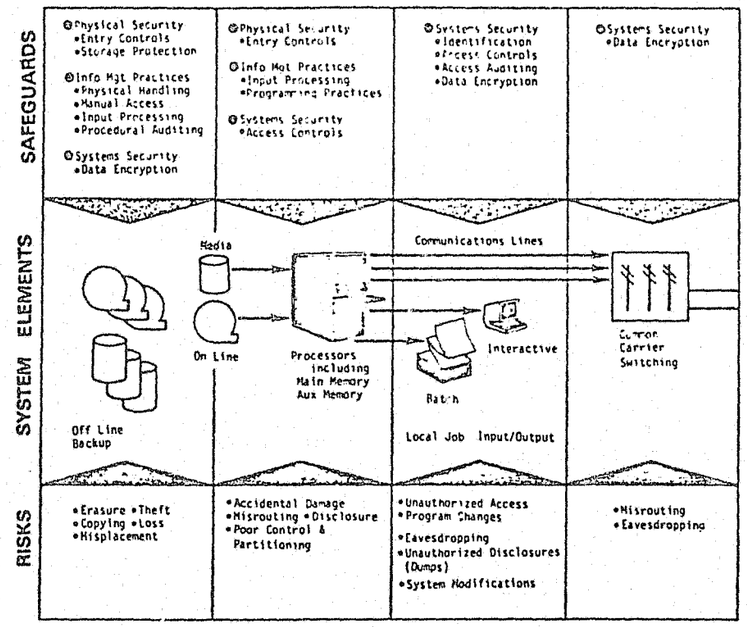

FIGURE 2. *Technical safeguards and data security risks.*

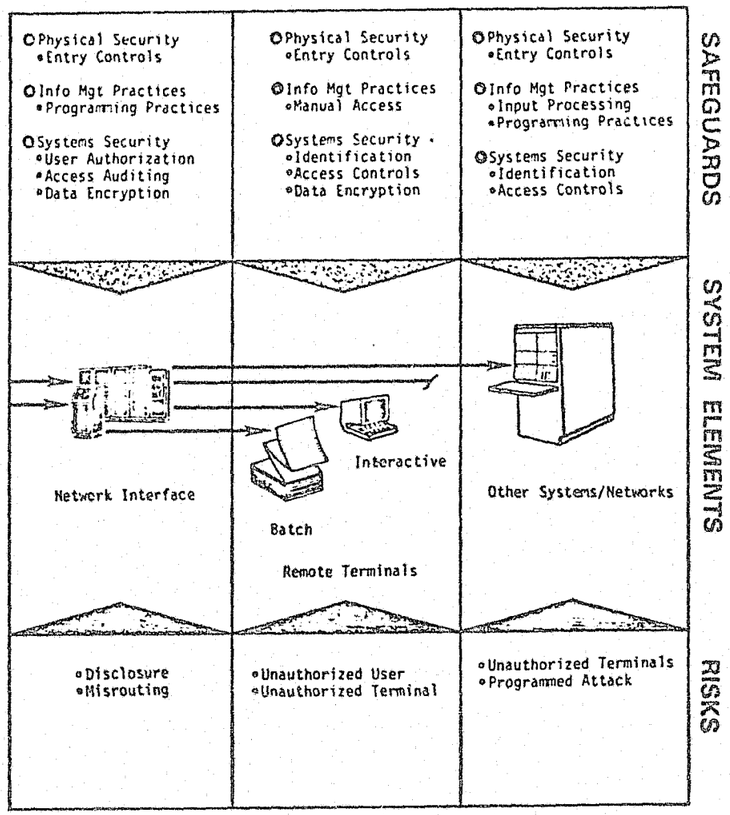

FIGURE 2—*Continued*

END