45596

AD/A-037 896

# PRIVACY AND SECURITY ISSUES IN INFORMATION SYSTEMS

REIN TURN, ET AL

RAND CORPORATION
SANTA MONICA, CALIFORNIA

JULY 1976

# PRIVACY AND SECURITY ISSUES IN INFORMATION SYSTEMS

Rein Turn
Willis H. Ware

July 1976





P-5684

The Rand Corporation
Santa Monica, California 90406



# PRIVACY AND SECURITY ISSUES IN INFORMATION SYSTEMS

Rein Turn and Willis H. Ware

Abstract -- A law now in effect in the United States requires protection of individual privacy in computerized personal information record-keeping systems maintained by the federal government. Similar laws apply in certain state and local governments. Legislation has also been introduced to extend the requirements for privacy protection to the private sphere. Central in privacy protection are the rights of an individual to know what data are maintained on him, challenge their veracity and relevance, limit their nonroutine use or dissemination, and be assured that their quality, integrity, and confidentiality are maintained. In all computer systems that maintain and process valuable information, or provide services to multiple users concurrently, it is necessary to provide security safeguards against unauthorized access, use, or modifications of any data file. This difficult problem has not yet been solved in the general case. Computer systems must also be protected against unauthorized use, disruption of operations, and physical damage. The growing number of computer applications involving valuable information or assets plus the growing number of criminal actions directed against computer applications and systems or perpetrated by using computers underscore the need for finding effective solutions to the computer security problem. In the future, concerns for privacy and security must become integral in the planning and design of computer systems and their applications.

*This paper was prepared for publication the November 1976 issue (the 25th anniversary issue) of the IEEE Transactions on Computers.

## I. THE EMERGING PROBLEMS

Privacy and security are problems associated with computer systems and applications that were not foreseen until well into the second half of the present computer age. Privacy is an issue that concerns the computer community in connection with maintaining personal information on individual citizens in computerized record-keeping systems. It deals with the rights of the individual regarding the collection of information in a record-keeping system about his person and activities, and the processing, dissemination, storage, and use of this information in making determinations about him. This last aspect is a long standing legal and social problem that has become associated with the computer field mainly because computerized record-keeping systems are much more efficient than the manual systems they have replaced, and because they permit linkages between record-keeping systems and correlations of records on a much greater scale than previously possible in manual systems. Thus, threats to individual privacy from manual record-keeping systems are potentially amplified in computerized systems.

Computer security includes the procedural and technical measures required (a) to prevent unauthorized access, modification, use, and dissemination of data stored or processed in a computer system, (b) to prevent any deliberate denial of service, and (c) to protect the system in its entirety from physical harm. The access control requirements are particularly important in time-shared and multiprogrammed systems in which multiple users are served concurrently--jobs processed concurrently must be prevented from interfering with each other and users must be prevented from gaining unauthorized access to each others' data or programs. When classified defense information is stored or processed in a system, the mutual

isolation of users is called the multilevel security problem: how can a system permit concurrent processing of information in different security classification categories, and concurrent use of the system by users who have different security clearances, while still guaranteeing that no classified information is leaked, accidentally or deliberately, to those who do not possess appropriate authorizations and security clearances.

Privacy and security emerged separately as problem areas in the computer field in the mid-1960s. The privacy cause célèbre was a recommendation in 1965 that a Data Service Center be established within the federal government to be a centralized data base of all personal information collected by federal agencies for statistical purposes [1]. This computerized system, also known as the National Data Bank, was to be used only for obtaining statistics in support of federal programs and decisions. The proposal received a strongly negative reaction from the Congress, news media, the legal community, and the public. Unfortunately, many of its critics have associated the envisioned threats to individual privacy and other freedoms that such a system was claimed to pose directly with the use of computers. Gathering of crib-to-grave dossiers on individuals and establishment of a comprehensive system of data surveillance were perceived to be direct consequences of the computer's presence.

Congressional hearings were held on the National Data Bank [2,3], and eventually the project was abandoned. Testimony given by computer specialists [4,5] at these and subsequent hearings exposed legislators, perhaps for the first time, to the potential of computer technology as a force to both cause and drive societal change and to the need for legislative action to surround computer applications that may produce harmful impacts



on society with appropriate legal safeguards. Since then, many papers and books have analyzed the privacy problem and offered solutions [6-9]; there is now a general consensus that the legislative approach, rather than reliance on self-policing by record-keeping agencies, is a preferred approach to solving the privacy protection problem in the United States. Different solutions have been proposed in other countries where there is a similar concern with threats to individual privacy [10,11].

Initial steps to solving the privacy problem in record-keeping systems have addressed specific sectors of society: the Fair Credit Reporting Act of 1971 grants certain rights to individuals who are data subjects in their relations with the financial credit reporting industry [12], the Privacy Act of 1974 requires privacy protection in record-keeping systems in the federal government [13], and the Family Educational Right and Privacy Act extends privacy protection to students' records in federally supported educational institutions [14]. Legislation generally similar to the Privacy Act has been enacted in Minnesota, Arkansas, and Utah and is pending in many others. At the present time, federal privacy bills encompassing the entire private sector and the criminal justice area are pending in Congress. The principles embodied in the already enacted and pending legislation and certain requirements they pose on record-keeping organizations are discussed in detail in Section II.

The first apprehension with computer security began in the 1950s with concern over degaussing of magnetic tapes and preventing dissemination of classified information via electromagnetic emanations. By the mid-1960s time-sharing and multiprogramming allowed computer systems to serve many users simultaneously, and on-line programming, job execution, and data file

manipulations could be performed from remotely located terminals. In such systems, as first discussed at the 1967 Spring Joint Computer Conference [15-17], security problems are different; there are many vulnerabilities which can be exploited by maliciously motivated users or by intruders from outside the system to perpetrate a variety of threats. Section III discusses these vulnerabilities and threats. Solutions to the physical security problem are now well in hand, but totally secure software and consequently, totally secure computer systems are still unattainable.



## II. PRIVACY PROTECTION PRINCIPLES

In the early 1970s, computerization of personal information record-keeping systems maintained by the federal, state, and local governments and in the private sector expanded rapidly. For example, it was emphasized during Congressional hearings on record-keeping systems maintained by the federal government that nearly two thousand such systems existed, containing hundreds of millions of personal records [18-20].

Proliferation of record-keeping systems has come to pass partly (a) because of the increasing size of the population plus the complex lives individuals lead; (b) because of the demand for services that society now makes on the government; (c) because of the need for improved efficiency in the conduct of government; and (d) because of the economics realizable in business. Contemporary computer technology provides society with the tool that it needs to accommodate growing information requirements, not only for the conduct of government but also for industry and commerce.

A study for the National Academy of Sciences [21] has demonstrated that, contrary to earlier beliefs, a great majority of organizations that have computerized their record-keeping systems have not significantly altered the data-collection and data-sharing policies followed in earlier manual systems. In particular, computerized record-keeping is still expensive enough generally to deter excessive collection of personal information.

### Privacy and Record-Keeping

Surrounded by record-keeping systems that contain extensive personal information about him, the citizen finds that he is increasingly in a

position of significant disadvantage in the balance of power between himself and the totality of data systems. He has given personal information to a record-keeping system for some purpose, usually because he expects in exchange some right, privilege, benefit, opportunity, or assurance of civil liberty. He expects that this information will be used for the purpose for which he gave it and in his best interest, certainly not in any way to his detriment. He does not expect to be annoyed, pressured, harassed, or harmed by its use.

An organization that holds personal data does so usually for some valid purpose; for example, it must administer a public assistance program, or operate a teaching institution, or maintain an inventory of some group of people such as property holders, customers, or persons wanted by the criminal justice system. Thus, the holder of personal information and the individual each have an interest in the proper use of such information. Neither should have unilateral control over its use; mutuality of control is appropriate.

This paper addresses personal privacy as it relates to the interface between an individual and any record-keeping system that holds personal information on him. Invasion of privacy implies that the holder of personal information has misused it to the detriment of one or more individuals, or has exploited it in some fashion other than for the purpose for which it was collected.

A pivotal aspect of the privacy issue is the present one-sided control that the "data owner" has over the use of personal information; in contrast, some argue that data on a given individual should belong to that individual and to no one else. Except in isolated categories of data, an individual has nothing to say about the use of information that he has given about himself or that has been collected about him. In particular, an organization



can acquire information for one purpose and use it for another, perhaps for its own bureaucratic end, perhaps for harassment, or perhaps for combining it with other data to create more extensive records on individuals. Moreover, the data owner can do this without consulting or informing the data subject. While recourse is now available to the individual in such sectors as the credit industry, federally controlled record-keeping systems, some educational institutions, and in some state and local governments, generally the private sector is not legislatively constrained.

## The Code of Fair Information Practices

Privacy is not a right explicitly enumerated in the United States Constitution, although it is in the California and Alaska constitutions. Furthermore, until recently the entire concept of privacy protection as it applies to personal information in record-keeping systems had not been developed. In related areas such as eavesdropping, wiretapping, and use of polygraphs, a series of court interpretations had applied various Amendments of the Constitution, such as the fourth amendment's right to security from unreasonable search and seizure. However, these were not readily and naturally applicable to information privacy.

A very different approach to individual privacy vis-a-vis record-keeping systems, in the context used in this paper (i.e., the rights of individuals regarding the collection, processing, storage, dissemination, and use of personal information), is the concept of a Code of Fair Information Practices. It was conceived by the Special Advisory Committee on Automated Personal Data Systems to the Secretary of the Department of Health, Education and Welfare [22], and rested on five principles that

had been talked about by many people but not succinctly and comprehensively considered as a whole prior to the HEW Committee.

Both the concept of a Code and its details are now widely used as the foundation of privacy legislation in the United States, and its applicability is being studied in other countries. The five basic principles of the Code are equally applicable to personal information record-keeping systems in the government and in the private sector:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for an individual to find out what information about him is on 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 from being used or made available for other purposes without his consent.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must guarantee the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

Legislation based on these principles would deter the misuse of personal information by stipulating that any deviation from the Code would be an abuse of personal information subject to criminal and civil sanctions, recovery of punitive and actual damages, and injunctive relief.



Privacy Safeguards

It was intended by the HEW Committee that the Code of Fair Information Practices would be implemented by a series of safeguards which collectively specify the preferred behavior and method of operation of record-keeping systems and which describe the rights and privileges of the individuals relative to them.

One set of safeguards would require an annual public notice that is intended to inform the public at large as to the name of a record system, its nature and purpose, its data sources, the categories of data maintained, the organizational policies and practices regarding data storage, and so forth. It would make visible the record-keeping practices of organizations.

A second set of safeguards would stipulate the behavior of an organization maintaining a personal data record system. The organization would be required (a) to identify a focal point to whom complaints could come; (b) to take affirmative action to inform its employees of the safeguards and to specify penalties for any infraction of them; (c) to take precautions against transferring identifiable personal information to data systems that may not include adequate safeguards; and (d) to maintain records with sufficient accuracy, completeness, timeliness, and pertinence as is relevant to their intended use.

A third set of safeguards gives the individual data subject certain rights: (a) When asked to supply personal data, he would be informed whether he is legally required to or may refuse to supply them; (b) he would be informed, upon his request, whether he is a subject in a given data system; (c) he would have the opportunity to inspect the record, to challenge it, and to cause corrections to be made; and (d) he would be

assured that data about him are used only for the stated purposes of the system.

Confidentiality of Statistical Data

In contrast to privacy, which refers to the rights of the individual vis-a-vis record systems, confidentiality implies that the data themselves must be protected, and that their use must be confined to authorized purposes by authorized people. Certain categories of personal information have a confidential status by statute. For example, the personal data gathered in the United States decennial census are required to be kept confidential by federal law [23]; this means that no individually identified census responses may be disseminated to anyone outside the Census Bureau, and even within the Bureau only specifically authorized employees are permitted access.

Most categories of personal information do not enjoy statutory protection. Disclosure of such information may be compelled by legal process, such as a subpoena issued by a court, search warrant, legislative committee, or other official body that has jurisdiction in the locality where the data are kept. Personal information gathered by educational institutions and by research projects in social, political, and behavioral sciences is susceptible to such procedures.

Absence of statutory confidentiality of personal information gathered for research purposes is a serious concern to researchers whose studies require the gathering of sensitive personal information. While the researcher may have the best of intentions as far as preventing any dissemination of identified information (and may even assure his respondents of its confidentiality), if faced with a subpoena he has the choice of either being in



contempt and suffering the penalties or of surrendering the data [24]. In either case his research project has been seriously damaged.

The Code of Fair Information Practices addresses this problem by seeking federal legislation to protect statistical reporting or research data against compulsory disclosure through the legal process. Such statutory protection should: (a) be limited to data identifiable with or traceable to specific individuals; (b) be specific enough to qualify for nondisclosure exemption under the Freedom of Information Act [25]; and (c) be applicable to data in the custody of all statistical reporting and research systems whether supported by federal funds or not. The federal law should be controlling; no state statute should interfere with the protection provided.

Whether or not general statutory confidentiality protection is provided for statistical reporting or research data, the Code would require that the data gathering organization:

1. Inform the individual whether he is legally required to supply the data requested or may refuse, and of any specific consequences for him, which are known to the organization, of providing or not providing such data;
2. Guarantee that no use of individually identifiable data will be made that is not within the stated purposes of the system as understood by the individual, unless the informed consent of the individual has been explicitly obtained; and
3. Guarantee that no data about an individual will be made available from the system in response to a compulsory legal process, unless the individual to whom the data

pertains has been notified of the demand and has been afforded full access to the data before they are made available in response to the demand.

Privacy Legislation

The principal privacy protection law now in force, the Privacy Act of 1974, applies to record-keeping systems maintained by federal agencies, except that intelligence, criminal justice, and law enforcement agencies and the National Archives either have exemptions or may seek exemption by formal rule-making procedures. The Act embodies the principles set forth in the Code of Fair Information Practices such as: (a) requiring that all agencies publish an annual notice on their record-keeping system; (b) requiring that an agency notify an individual, upon his request, of the existence of any records of personal information on him; (c) granting the individual the right of access to his records and their correction or amendment; (d) requiring that the agency obtain prior approval from the individual concerned for any nonroutine use or dissemination of his records; and (e) providing penalties, both criminal and civil, that can be levied for failure to comply.

In addition, the Privacy Act established a Privacy Protection Study Commission with a charter to study record-keeping systems in governmental and private organizations not yet covered by the Privacy Act, in order to recommend whether the Act, and which of its provisions, should be extended to cover these systems.

Pending in Congress is a bill, H.R. 1984, which would extend the Privacy Act to record-keeping systems in the private sector and would strengthen numerous requirements of the present Act. For example,



(a) notices would have to be published in local or regional news media that are most likely to reach the largest number of data subjects; (b) individuals would have to be notified of their records on the agency's own initiative; (c) the use of Social Security numbers, or any other universal identifiers, would be prohibited if not required by statute or unless given permission by Congress; (d) the only exemptions would be active criminal investigation files, data systems maintained by the news media, and certain mailing lists. Penalties for noncompliance would be strengthened, and a Federal Privacy Board would be established to oversee enforcement of the Act.

Implementation and Costs

There are a number of procedural and technical ways of implementing the privacy protection requirements of the Privacy Act of 1974, state privacy laws, and pending privacy protection bills. For example, organizations that are in regular correspondence with individuals in their record-keeping systems can use such means for notifying them of the existence of records. Requirements of the Privacy Act to assure that records are "accurate, complete, timely, and relevant for agency purposes," and that the agency "establish the appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records" involve three categories of technical safeguards: information management practices, physical security procedures, and data security controls within the system and its communications. No part of a system by itself is likely to offer protection against all risks of privacy violation, but by careful selection of safeguards that reflect the needs of the data system being considered, the level of protection can usually be improved significantly at reasonable

cost [26]. Safeguards for data security are discussed briefly in the following section.

The cost of implementing privacy safeguards depends on the details of the record-keeping system and the implementation [27,28]. Initial cost includes the analysis, design, and implementation of the protection system safeguards; acquisition of protection-oriented equipment; improvement of data handling practices and generation of the necessary software; conversion of the data bases to make provisions for protection-oriented data fields; and management adjustments. The operational costs include salaries of employees performing protection-oriented tasks, the cost of computer resources for protection-oriented processing and communication task, and the administrative cost of privacy protection.

Other protection-related costs may be less visible. For example, protection requirements may reduce the availability of a record-keeping system to other users, as well as reducing the system's throughput and efficiency. If such reductions are significant, the record-keeping system may be unable to meet its peak inquiry-handling or processing demands, and may need additional or faster processors or additional storage configuration capacity. In this respect privacy protection may be in conflict with the usual goals of a system's manager and users.

No information is yet available on the cost experience of federal or state agencies under the Privacy Act of 1974; but it has been estimated that the initial costs are approximately $100 million and the recurring costs $200 million. On a per-capita basis, these costs are quite reasonable--roughly a dollar for each person in the country. However, much higher costs have been estimated for the private sector, and certainly



the basis over which to spread the costs is much smaller. Clearly, legislatures must take care not to specify protection requirements that would entail unreasonable implementation costs or that may be even technically infeasible.

## III. COMPUTER SECURITY

In addition to supporting legally mandated privacy protection requirements, there are other compelling reasons for maintaining computer and data security. Computers in the federal government process classified information on national defense policies, systems, and plans. In business and industry, valuable information on new product development, marketing, finances, and planning are kept in computer systems. The financial community is automating banking and funds transfer systems; Electronic Funds Transfer Systems (EFTS) will eventually replace a large percentage of financial documents with electronic signals and magnetization patterns.

### Computer Abuse

Computerization of daily business operations has provided new opportunities and new means for such white-collar crimes as embezzlement, falsification of records, fraud, and larceny. Case histories demonstrate employees who manage or design data systems, write application programs, or operate the equipment have recognized opportunities for criminal acts [29,30]. Abuses that the computer makes especially easy are payments for fictitious purchases or to ficticious employees, manipulation of credit levels, and deposits of unauthorized payments into various accounts. Consolidation of record-keeping systems into computerized systems creates highly centralized, easily identifiable targets for disruption, sabotage, or fraudulent manipulation. Table 1 summarizes a history of computer abuse incidents.

As previously noted, computer security includes safeguards to (1) protect a computer-based system, including its physical hardware, personnel, and data against deliberate or accidental damage; (2) protect the system

Table 1

REPORTED CASES OF COMPUTER ABUSE[a]

| Year | Financial Fraud | Theft of Information | Unauthorized Use | Vandalism | Total |
|---|---|---|---|---|---|
| 1969 | 3 | 6 | 2 | 4 | 15 |
| 1970 | 10 | 5 | 10 | 8 | 33 |
| 1971 | 23 | 19 | 6 | 6 | 54 |
| 1972 | 16 | 17 | 18 | 15 | 66 |
| 1973 | 26 | 20 | 11 | 11 | 68 |
| 1974 | 25 | 15 | 12 | 7 | 59 |
| 1975 | 26 | 7 | 4 | 6 | 43 |
| Totals | 129 | 89 | 63 | 57 | 338 |

[a] As of January 1976. Data for 1974 and 1975 are still incomplete. Personal communication from Donn Parker, Stanford Research Institute, Menlo Park, California

against denial of use by its rightful owners; and (3) protect information or data against divulgence to unauthorized recipients. Th[illegible]ts that must be averted include natural disasters, riots, equipment failures, negligent or maliciously motivated employees and users, and external intruders.

Although manual record-keeping systems and data files are subject to similar threats, certain characteristics of information storage and processing in computer systems make threats to them more serious. First, information is stored in forms not directly readable by users, e.g., magnetization, voltage-levels. They can be changed without a trace of evidence unless comprehensive audit trails have been incorporated into the system design. Computerized records do not have signatures or seals to verify authenticity or to distinguish copies from originals, and they can be manipulated electronically from terminals remote from the physical storage of the data. Transactions can be performed automatically at high speed without human monitoring or intervention. Finally, processing rules are expressed as programs stored in the same devices and in the same manner as the data; they too can be changed without trace. While processing programs are difficult to validate, a properly designed and implemented computerized information system can control errors and manage access to the records much more effectively than can any manual record-keeping system, provided such controls have been included in the design specifications.

Security Safeguards

It is now reasonably well understood how to provide computer security [15,16,31]. In particular, it is understood that:

1. Physical safeguards such as locks, fire protection, water protection, and so forth to prevent physical damage to the equipment and its associated information.



2. Computer hardware safeguards such as memory protect, are essential to implement an access control mechanism between user and computer file and to isolate users from one another.
3. Software safeguards such as a file access control scheme must be provided to create, in conjunction with hardware, a protective barrier between a user and data files to which he is not authorized while permitting his access to those which he is.
4. Communication safeguards must be provided when necessary to assure secrecy of information when in transit over communication channels.
5. Personnel safeguards such as background checks, bonding, training, and disciplinary actions are required to deter potential leakage of information due to an individual's actions.
6. An administrative and management overlay must be created that oversees all aspects of the security safeguard system; inspects, tests and audits them; and controls movement of people, magnetic discs, magnetic tapes, paper, etc.

Thus, within a conceptual security fence one finds the computer with its software and application programs, communication circuits, terminals, data files and support personnel.

The techniques for providing physical security to the computer system are in hand [32,33]. A variety of equipment and techniques exist for controlling fires in computer rooms, preventing unauthorized physical access,

providing safe storage, and the like. Nevertheless, their application in a given system requires careful analysis of the threat and engineering. For example, a ceiling water sprinkler system may not be appropriate in a computer room; and although a tear gas dispensing system may deter a rioting mob, it can also corrode computer circuitry.

A different set of techniques deals with protection of programs and data within the computer system against unauthorized access or modification. Such access may be obtained accidentally due to hardware or software errors, or by intent as a result of a preplanned penetration operation. In the latter case the ability of a penetrator to gain access to protected resources depends on the sophistication of the security safeguards employed, as well as on the structure of the computer system and the services it provides to its users. For example, a remotely accessible, time-shared system which permits users to submit their own assembly language programs offers more opportunities for penetration than a system in which users cannot submit programs and are limited to performing a fixed set of transactions. Security tests have demonstrated that at present there exist no resource-sharing computer systems that do not yield to sustained penetration attempts [34].

Data security techniques are intended to counter threats that can be reasonably expected to be directed against the system or, if absolute prevention is impossible or impractical, at least to increase the cost of penetration and the risk to the penetrator to levels where the possible profit from penetration is no longer advantageous. The methodology for performing threat analyses, assessing the level of the system's security, and designing a cost-effective security system is still being developed, but guidelines are available [26,33].



The objectives of implementing security techniques in computer hardware and software include the following:

1. Isolation of users and their processes (programs in execution) from each other and from the system's supervisory programs to prevent interference with each other or with the supervisor and to prevent a user from capturing control of the system;
2. Positive identification of all users and authentication of their identities; attachment of unforgeable identifiers to all programs being processed;
3. Total control by the system's supervisory program over all shared system resources (memory space, data files, subroutines, input-output devices, communications, etc.) and over all processes;
4. Concealment of information on removable storage media and in communication channels by encryption techniques;
5. Implementation of effective integrity controls and auditing procedures to assure that security safeguards operate correctly and that users follow security procedures.

Techniques for implementing security objectives are briefly discussed below; details can be found in recent literature [35].

Isolation and Identification

A conceptually simple way to isolate users is to process their programs one at a time, completely erasing any portion of memory that has been used before processing the next job. This approach is still practiced in

processing classified government data, but it is unnatural, wasteful in modern resource-sharing systems, and does not exploit third-generation capabilities. An elementary isolation technique is to bound the memory space assigned to a user and test each memory reference for compliance with the bounds.

A major advantage of contemporary computer systems is the ability of users to share programs and data among themselves. However, the owners of shared resources must be able to specify to the system who is to access data and what processing actions each may take. In return, the system must be able to enforce rigid rules not only under static predetermined conditions, but also under dynamic conditions when authorization changes occur frequently. In a dynamic situation, an authorized user may generate new processes and data files and wish to pass selected access rights to others, to retract previously granted rights, or to specify the rights-passing conditions within the new processes themselves. Clearly, management of access rights is a complicated task that must be implemented in the operating system software. Techniques for this are discussed in Ref. 35.

No access control technique can work effectively without an ability to identify users and authenticate the identification. Commonly used identification techniques include a user name, person number, or account number as supplied by the user. Authentication may be based on something the user knows, is, or has. The first category includes passwords, combinations to locks, or some facts from a person's background. Passwords are widely used and can be quite effective if they are properly chosen, managed, and safeguarded. They should not be (a) easy to guess, (b) excessively long



or complicated, or (c) printed out at terminals; and (d) they should be changed frequently.

Authentication can also be based on automated recognition of some hard-to-forge physical characteristic of the individual (e.g., fingerprints, voice print, signature, or hand dimensions). Automated recognition techniques are still being developed and so far tend to be expensive. In the third category, "something a person has," are computer-readable badges and cards. Typically, they contain authentication information (which should be unknown to the individual) on a magnetic strip part of the card, which can be encrypted to prevent forgeries. If possession by users is mandatory, and penalties are levied for noncompliance, careless handling would be sharply reduced.

Encryption

Cryptographic techniques can be used in communication links between computers and between computers and terminals to protect information from interception by wiretapping, or capture and modification at illicit terminals or computers that could be surreptitiously inserted in the system. Such threats are extraordinarily and ominously real in computer networks handling monetary transactions, such as the proposed EFTS. Historically, crytographic techniques were developed for concealment of natural language messages, but the basic principles are also applicable for protection of computer data [36-38]. There are a number of differences, however, between natural language text and computer data which both enhance and diminish the protection provided. For example, data in computers are mostly numerical values, codes, names and addresses of individuals, or statements in artificial programming languages. These tend to have more uniform character

frequency statistics than natural languages, thus reducing the effectiveness of such cryptanalytic processes as frequency analyses. On the other hand, computer data and records tend to have rigid formats, follow strict syntactic rules, and large amounts of encrypted material are available; all tend to help cryptanalytic efforts.

Given such differences and the availability of computers themselves for cryptanalysis, standard cryptographic techniques are not overly effective [39]. Fortunately, rapidly decreasing costs of digital hardware are now making economical new, much more complex and much more effective techniques, such as the standard encryption algorithm recently proposed by the National Bureau of Standards [40]. The NBS algorithm operates on 8-byte blocks of data by applying a long sequence of key-dependent substitutions, transpositions, and nonlinear operations to thoroughly mix the original bits. Its implementation in software is rather inefficient, but it will be acceptably fast and economical if manufactured as a microelectronic hardware chip using large scale integration (LSI) manufacturing methods. It is to be expected that future computers will use similar cryptographic devices to protect information stored in data bases.

Integrity and Auditing

A system of security safeguards is effective only if it is correctly designed and implemented, operates correctly thereafter, and is constantly monitored. A major source of vulnerabilities in resource-sharing systems is the operating system software which may contain hundreds of program modules and hundreds of thousands of instructions. It is impossible to design and implement such systems without risking many design flaws and implementation errors. Although a vast majority of such flaws and errors



will be removed in debugging phases, many will remain undetected for long periods; indeed, errors are still being found in operating systems that have been in use as long as ten years. Some flaws may provide a way for disabling or circumventing the security system by knowledgeable penetrators [31,34] and are, therefore, of special concern.

Software shortcomings are, of course, a general problem in producing reliable systems, but security requirements add a new dimension. Not only should programs correctly perform all tasks they are designed for, but they should not do anything they are not intended to do. Verifying that a program satisfies such a stringent requirement is very difficult, and may be possible only by formal correctness proofs. Unfortunately, very little progress has been made in developing practical program proving techniques, or of exhaustive testing or verification.

In the absence of totally effective security safeguards in contemporary computer systems, various auditing procedures are used to discourage the curious or slightly larcenous users—the expert penetrators will not be thwarted—and to maintain control over the system [41]. Typically, records are made of all jobs processed in the system, all log-ons at on-line terminals, accesses to files, exception conditions detected by the system, and the like. If an audit log is properly designed, it can permit tracing anamalous user actions in the system and, thus, establish accountability through ex post facto analysis; moreover, active and dynamic audits can intercept a penetration effort in progress.

In present systems, real-time threat monitoring is implemented at a very primitive level. For example, counts are made of the number of consecutive times a user fails to provide a correct password and, if a preset

threshold is exceeded, the user is automatically disconnected. More sophisticated threat monitoring requires an ability to characterize security violations in terms of measureable system variables, an ability to distinguish penetration attempts from other unusual but legitimate data processing activities, and the ability to instrument the system to collect needed information without unacceptable increases in the system's overhead.



## IV. CONCLUDING REMARKS

We have presented a broad overview of privacy and security in computer systems--two topics important in the design, operation, and use of contemporary computer systems that will become even more important in the future. Space did not permit detailed treatment of technical aspects; these are available in the cited literature.

A ten-year period of alerting the American public to the latent dangers posed to their individual rights and freedoms by computerization of record-keeping systems has ended with the enactment of the Privacy Act of 1974. With this landmark legislation, we entered an era of active resolution of the privacy problem. Extension of privacy protection to record-keeping systems maintained by criminal justice and law enforcement agencies of state and local governments, and by private industry and institutions is the next order of business.

We must recognize, however, that the right of privacy vis-à-vis record-keeping systems is not more important than other individual rights that may be supported and strengthened by the same record-keeping systems. In many cases the objectives in providing privacy are in consonance with other rights, but at times they conflict. There is a central conflict between the legitimate need of public and private institutions for information about people and the need of individuals to be protected against harmful uses of information. There is also a conflict between an individual's desire for privacy and society's collective need to know about and to oversee government's operations. Furthermore, since privacy safeguards can delay access to information needed for making determinations about an individual or can increase the associated costs, privacy can be in conflict even with the

individual's own interests. Yet it has been said that "freedom is what privacy is all about," and that without privacy protection the very existence of massive record systems in the government will have a chilling effect on citizens' exercise of their rights of freedom of expression and of petitioning the government. Thus, it will not be easy to strike the right balance among the many dimensions of this issue. The Privacy Act of 1974 is a starting point on a learning curve which through amendments, court decisions, and new privacy laws, will hopefully lead toward such a balanced solution. Numerous organizations, study groups, and especially the Privacy Protection Study Commission established by the Privacy Act of 1974 are working toward this end.

Techniques for providing data security are evolving rapidly, but much research and development remains to be carried out. At present these efforts are concentrating on software--the design of provably secure operating systems or operating system kernels for implementing the access control function. Attention is also being focused on hardware approaches to security--new architectures that reduce the need for resource sharing and that provide special access control hardware. Concepts such as data base machines and security machines are already emerging. It is almost certainly clear that a balanced approach between hardware, software, and procedures will provide the most effective security safeguards.

Legal provisions already exist to require data security in personal information record-keeping systems. Valuable organizational assets are increasingly represented by records in computer data bases rather than by hardcopy documents; systems such as the Electronic Fund Transfer offer high pay-off opportunities for computer crime of various kinds. As statistics



on computer abuse show, the perpetrators of criminal acts are rapidly moving upward on a learning curve of their own; thus, in this environment it is a serious challenge for the computer profession to devise effective solutions now. We cannot wait for a leisurely sojourn through the next 25-year segment of the computer era.

REFERENCES


1. *Report of the Committee on the Preservation and Use of Economic Data to The Social Science Research Council* (Richard Ruggles, Chairman), Washington, D. C., 1965.

2. *Special Inquiry on Invasion of Privacy*, Hearings, House Committee on Government Operations, Special Subcommittee on Invasions of Privacy, 89th Congress, Parts 1 and 2, U.S. Government Printing Office, Washington, D. C., 1966.

3. *Computer Privacy*, Hearings, Senate Committee on the Judiciary, Special Subcommittee on Administrative Practice and Procedure, U. S. Government Printing Office, Part I: 1967, Part II: 1968.

4. P. Baran, *Communications, Computers and People*, The Rand Corporation, Santa Monica, California, P-3235, November 1965.

5. P. Armer, *Privacy Aspects of the Cashless and Checkless Society*, The Rand Corporation, Santa Monica, California, P-3822, April 1968.

6. A. F. Westin, *Privacy and Freedom*, Atheneum, New York, 1967.

7. A. R. Miller, *Assault on Privacy: Computers, Data Banks and Dossiers*, University of Michigan Press, Ann Arbor, Michigan, 1971.

8. A. Harrison, *The Problem of Privacy in the Computer Age: An Annotated Bibliography*, The Rand Corporation, Santa Monica, California, Volume I: RM-5495-PR/RC, December 1967; Volume II: RM-5495/1-PR/RC, December 1969.

9. M. K. Hunt and R. Turn, *Privacy and Security in Databank Systems: An Annotated Bibliography, 1970-1973*, The Rand Corporation, Santa Monica, California, R-1361-NSF, March 1974.

10. F. W. Hondius, *Emerging Data Protection in Europe*, North-Holland Publishing Company, Amsterdam, 1975.

11. *Privacy and the Computers, A Report by Department of Communications and Department of Justice*, Information Canada, Ottawa, Canada, 1972.

12. Fair Credit Reporting Act of 1971, Title 15, U.S. Code, Section 1681.

13. *Privacy Act of 1974*, Title 5, U. S. Code, Section 557a (Public Law 93-579, December 31, 1974).

14. Family Educational Rights and Privacy Act, Title 5, P.L. 930380, 1974.

15. W. W. Ware, "Security and Privacy in Computer Systems," *AFIPS Conference Proceedings*, Vol. 30, 1976 SJCC, pp. 279-282.

16. H. E. Petersen and R. Turn, "System Implications of Information Privacy, *AFIPS Conference Proceedings*, Vol. 30, 1967 SJCC, pp. 291-300.





17. B. Peters, "Security Considerations in a Multi-Programmed Computer System," *AFIPS Conference Proceedings*, Vol. 30, 1967 SJCC, pp. 283-290.

18. *Federal Data Banks, Computer and The Bill of Rights*, Hearings, Senate Committee on the Judiciary, Constitutional Rights Subcommittee, 92nd Congress, First Session, 1971.

19. *Federal Data Banks and Constitutional Rights, A Study in 6 Volumes*, Senate Committee on the Judiciary, Subcommittee on Constitutional Rights, 1974, 93rd Congress, 2nd Session.

20. *Privacy--The Collection, Use and Computerization of Personal Data*, Joint Hearings, Ad Hoc Subcommittee on Privacy and Information Systems, Senate Committee on Government Operations, and Subcommittee on Constitutional Rights, Senate Committee on the Judiciary, 93rd Congress, 2nd Session, 1974.

21. A. F. Westin and M. A. Baker, *Databanks in a Free Society*, Quadrangle Books, New York, 1972.

22. *Records, Computers, and the Rights of Citizens, A Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (W. H. Ware, Chairman), U. S. Department of Health, Education, and Welfare, Washington, D. C., 1973.

23. U. S. Code, Title 13, Section 9.

24. R. Nejelski and L. M. Lerman, "A Researcher-Subject Testimonial Privilege: What to Do Before the Subpoena Arrives?", *Wisconsin Law Review*, No. 4, 1971, pp. 1085-1148.

25. U. S. Code, Title 5, Section 552.

26. *Computer Security Guidelines for Implementing the Privacy Act of 1974*, FIPS Publication No. 41, National Bureau of Standards, Washington, D. C., May 30, 1975.

27. R. Turn, "Cost Implications of Privacy Protection in Databank Systems," *Data Base*, Spring 1975, pp. 3-9.

28. R. C. Goldstein, *The Cost of Privacy*, Honeywell Information Systems, Brighton, Massachusetts, 1975.

29. D. B. Parker, "Computer Abuse Perpetrators and Vulnerabilities of Computer Systems," *AFIPS Conference Proceedings*, Vol. 45, 1976, NCC, pp. 65-73.

30. B. Allen, "Embezzler's Guide to the Computer," *Harvard Business Review*, July-August 1975, pp. 79-79.

31. J. P. Anderson, "Information Security in a Multi-User Computer Environment," *Advances in Computers*, Vol. 12, Academic Press, New York, 1972, pp. 2-36.

32. *Guidelines for Automatic Data Processing: Physical Security and Risk Management*, FIPS Publication No. 31, National Bureau of Standards, Washington, D. C., 1974.

33. *AFIPS System Review Manual on Security*, AFIPS Press, Montvale, New Jersey, 1974.

34. T. Alexander, "Waiting for the Great Computer Rip-Off," *Fortune*, July 1974, pp. 143-150.

35. J. H. Saltzer and M. C. Schroeder, "Protection of Information in Computer Systems," *Proceedings of the IEEE*, September 1975, pp. 1278-1308.

36. R. Turn, "Privacy Transformations For Databank Systems," *AFIPS Conference Proceedings*, Vol. 42, 1973 NCC, pp. 289-601.

37. H. Feistel, W. A. Notz, and J. L. Smith, "Some Cryptographic Techniques for Machine-to-Machine Data Communications," *Proceedings of the IEEE*, November, 1975, pp. 1545-1554.

38. H. S. Bright, and R. L. Enison, "Cryptography Using Modular Software Elements," *AFIPS Conference Proceedings*, Vol. 45, 1976 NCC, pp. 113-123.

39. B. Tuckerman, *A Study of the Vigenere-Vernam Single and Multiple Loop Enciphering Systems*, Report RC-2879, IBM Research Laboratory, Yorktown Heights, New York, 1970.

40. "National Bureau of Standards Encryption Algorithm," *Federal Register*, March 17, 1975.

41. E. G. Jancura and A. H. Berger (Eds.), *Computers: Auditing and Control*, Auerbach Publishers Inc., Philadelphia, 1973.

END