Computers and Privacy: A Survey

LANCE J. HOFFMAN

Stanford Linear Accelerator Center, Stanford University, Stanford, California*

The problem of access control and privacy in computer systems is surveyed in terms of existing systems and current proposals. A review of suggested legal and administrative safeguards is given The bulk of the discussion deals with the current technology, its limitations, and some additional safeguards which have been proposed but not implemented. Finally, a few promising computer science research problems in the field are outlined A partially annotated bibliography of literature in the area is included.

Key words and phrases: privacy, access control, confidentiality, privacy transformations, social implications, public utility, time-sharing, legislation, regulation, professionalism, access management, data bank, dossiers, ethics, authority items

CR categories: 2.11, 2 12, 2 2, 2.3, 4.30

THE PRIVACY PROBLEM

In the last several years, computer systems used as public utilities have moved from dream to reality. There are now a large number of multiterminal, on-line, time-sharing systems in both commercial and academic environments [13, 15, 42, 49, 50]. Many people fully expect a public "data bank grid" to come into existence in the very near future; they point out [47] that "it is as inevitable as the rail, telephone, telegraph, and electrical power grids that have preceded it, and for the same reasons. It is much less expensive and more efficient to share information than to reproduce it."

Unfortunately, current information networks do not have adequate safeguards for the protection of sensitive information. However, since the benefits derivable from automation of large data banks are so great, pressure in some circles [17, 20, 33, 34] is building up to "computerize now." Automation offers benefits in both economy and performance over many current systems.

* Computation Group. This work was supported by the US Atomic Energy Commission

Social scientists and statisticians, for example, have suggested the creation and maintenance of a national data bank [34]. Its use would remedy many defects of current files and procedures which result in information unresponsive to the needs of vital policy decisions. Some of these defects, as pointed out by Dunn [21] are:

—Important historical records are sometimes lost because of the absence of a consistent policy and procedure for establishing and maintaining archives.

—The absence of appropriate standards and procedures for file maintenance and documentation lead to low quality files that contain many technical limitations in statistical usage.

—Many useful records are produced as a by-product of administrative or regulatory procedures by agencies that are not equipped to perform a general purpose statistical service function.

—No adequate reference exists that would allow users to determine easily whether or not records have the characteristics of quality and compatibility that are appropriate to their analytical requirements.

—Procedures for collecting, coding and tabulating data that were appropriate when developed now lead to some incompatibilities in record association and usage required by current policy problems and made possible by computer techniques.

—There are serious gaps in existing data records

CONTENTS

that stand in the way of bringing together records of greatest relevance for today's problems

—The need to by-pass problems of record incompatibility in developing statistics appropriate for policy analysis, places severe strains upon regulations restricting the disclosure of information about individuals. Technical possibilities for using the computer to satisfy these statistical requirements without in any way violating personal privacy have not generally been developed and made available by the agencies

To take advantage of the economies and capabilities of the computer, governmental agencies and private organizations such as credit bureaus are making use of computer-based personal dossier systems. The New York State Identification and Intelligence System (NYSIIS) provides rapid access to criminal histories, stolen property files, intelligence information, etc., for use by [26] "qualified agencies." Santa Clara (California) County's LOGIC system [17] will include a person's name, alias, social security number, address, birth record, driver and vehicle data, as well as other data if the person has been involved with the welfare or health departments, the district attorney, adult or juvenile probation, sheriff, court, etc. Other municipalities have created similar systems.

These large data banks will make it easy for the citizen in a new environment to establish "who he is" and thereby to acquire quickly those conveniences which follow from possession of a reliable credit rating and a social character acceptable to his new community. At the same time, commercial or governmental interests will know much more about the person they are dealing with. We can expect a great deal of information about social, personal, and economic characteristics to be supplied voluntarily—often eagerly—in order to enjoy the benefits of the economy and the government [40].

There is another side to the coin, however. Since much more information on a person will be stored in the same place, less effort will be necessary to acquire certain "sensitive" data. If insufficient consideration is given to access control and to keeping the price of sensitive information "high enough," the temptation to demand

or to buy this information will increase, since these new systems could be illicitly probed for derogatory information on an individual [59].

Systems with insufficient input checking might be given false and slanderous data about a person which, when printed out on computer output sheets as the result of an inquiry, looks quite "official" and hence is taken as true. "On the horizon in technology is a laser scanning process that would enable a twenty-page dossier to be compiled on each of the 200 million citizens of the United States. Such information could be stored on a single plastic tape reel. Under such conditions it might be cheaper to retain data than to discard it." [9] Clearly, we must decide what information to keep and when to keep it. As Paul Baran points out [4], we face a balance problem. How do we obtain the greatest benefit from computer data banks with the least danger?

LEGAL AND ADMINISTRATIVE SAFEGUARDS

The problem of controlling access to computer files—how to safeguard the processes of inputting to and retrieving from computer data banks—has recently gained more and more attention from concerned citizens. We examine some of this new interest in this section, deferring mention of the technical solutions to the next section.

Bauer has given a brief but sound discussion of policy decisions facing the designers of a computer data bank and has pointed out [6] that we now have the "special but fleeting opportunity . . . to explore the issue of privacy with objectivity and in some leisure. . . . the public's fears of dossier-type police information systems have been thoroughly aroused; left unchecked they may become so strong as to in fact prevent the creation of any publicly supported information systems. The reactions to proposals for a Federal data center are a case in point. Were such blanket prohibitions to be imposed the development of socially useful information-sharing would be enormously impeded. Furthermore, without public trust, information systems could well be fed so much false, misleading or incomplete information as to make them useless. Thus it becomes imperative not only to devise proper safeguards to data privacy, but also to convince the public and agencies which might contribute to a system that these safeguards are indeed being planned, and that they will work."

Fortunately, the Federal Government is aware of the computer privacy problem and has been unreceptive, even hostile, to proposals which do not consider the costs and effectiveness of safeguards necessary to protect privacy in a centralized data bank [56, 57, 68]. Most states, however, lag seriously in awareness of contemporary data processing capabilities and techniques. A few of the more highly computerized areas are, however, trying to approach the idea of regional data banks in a rational manner. At least one state (California) has an intergovernmental board on automatic data processing which has solicited and received comments from concerned members of the technical community on confidentiality and the invasion of privacy.

As Senator Sam J. Ervin, Jr. has pointed out [24], the threat to privacy comes from men, not machines; it comes from the motives of political executives, the ingenuity of managers, and the carelessness of technicians. Too often, he says, an organization may seize upon a device or technique with the best intentions in the world of achieving some laudable goal but in the process may deny the dignity of the individual, the sense of fair play, or the right of the citizen in a free society to the privacy of his thoughts and activities.

"The computer industry, the data processing experts, the programmers, the executives—all need to set their collective minds to work to deal with the impact of their electronic systems on the rights and dignity of individuals.

"While there is still time to cope with the problems, they must give thought to

the contents of professional ethical codes for the computer industry and for those who arrange and operate the computer's processes.

"If self-regulation and self-restraint are not exercised by all concerned with automatic data processing, public concern will soon reach the stage where strict legislative controls will be enacted, government appropriations for research and development will be denied. And the computer will become the villain of our society. It is potentially one of the greatest resources of our civilization, and the tragedy of slowing its development is unthinkable." [24]

Though Senator Ervin gave that speech on 1 May 1967, so far only Chairman Watson of IBM, of all the computer manufacturers, has commented publicly on the subject [60]. The Washington, D.C. Chapter of the ACM has gone on record as opposing the creation of a national data bank until the proposers can show that [58] "such a system is still economically attractive under the legal and technical constraints necessary to protect individual liberties in the American society." (It has been alleged, however, that this vote reflects the views of a minority of that chapter's members and cannot necessarily be taken to represent the view of the chapter.)

We often forget that no "right to privacy," similar to the "right to freedom of speech" or the "right to vote," exists in the Constitution. Thus, the amount of privacy an individual is entitled to and the situations in which that privacy may be violated vary according to the whim of a particular court or legislative body [24, 36, 62]. Prosser, of the University of California School of Law at Berkeley, has compiled an excellent review of this subject [45].

Recently, significant efforts have been made to create a more satisfactory situation. In 1966 John McCarthy suggested a "computer bill of rights." Some of the rights he proposed were these [38]:

—No organization, governmental or private, is allowed to maintain files that cover large numbers of people outside of the general system.

—The rules governing access to the files are definite and well publicized, and the programs that will enforce these rules are open to any interested party, including, for example, the American Civil Liberties Union.

—An individual has the right to read his own file, to challenge certain kinds of entries in his file and to impose certain restrictions on access to his file

—Every time someone consults an individual's file this event is recorded, together with the authorization for the access.

—If an organization or an individual obtains access to certain information in a file by deceit, this is a crime and a civil wrong. The injured individual may sue for invasion of privacy and be awarded damages.

Additional suggestions have been made concerning legislative methods of safeguarding privacy. In 1967 the United States government proposed a Rights to Privacy Act banning wiretapping and electronic eavesdropping. (In 1968, however, the pendulum swung the other way and the United States Congress passed a "safe streets" and crime-control bill which granted broad authority for wiretapping and eavesdropping, even without a court order, for a limited period of time.)

Even if a statute controlling access to sensitive information in files of the Federal Government were passed, the computer privacy problem would still be a long way from solved. A threat which is possibly even more serious is the misuse of data in the files of private organizations or in the files of state or local governments. Medical records in the files of hospitals, schools, and industrial organizations contain privileged information. When these records are kept in a computer-based system, there must be control over access to them. Some disconcerting examples of what has happened when controls are lax are mentioned in a paper by Baran [4].

California has recently passed into law legislation which (1) recognizes an individual's right of privacy, and (2) recognizes computerized data in state files as "public records." This legislation may well prove to be a landmark in the fight to establish a "right to privacy" and would seem to guarantee the right of an individual to read his own file.

The licensing or "professionalization" of (at least some) computer scientists, programmers, and operators seems to be the most frequent suggestion in the papers on computer privacy which are not written solely for computer scientists. In addition to Ervin (see above), advocates of this measure include Michael [7], Brictson [10], and Ramey [47]. Parker has been the main supporter of the ACM Guidelines for Professional Conduct in Information Processing [41], but Brictson makes the best argument the author has seen for these to date [10]. With such current and potential outside interest in professional conduct of computer people, there has been very little published discussion about these matters. In view of Senator Ervin's unsettling predictions (above), perhaps the computer community should give these problems more attention than it has to date.

This concludes the discussion of legal and administrative safeguards for the protection of sensitive information. We can now turn our attention to the technical solutions that have been proposed.

TECHNICAL METHODS PROPOSED TO DATE

Access Control in Conventional Time-Sharing Systems

Various technical methods for controlling access to the content of computer memories have been suggested. In this discussion these methods are broken up into two categories—those which are necessary for proper operation of a time-sharing system and those which enhance the privacy of data in a shared system.

Methods necessary for a properly operating time-sharing system. First let us consider the controls required in any time-sharing system. A means must be provided to lock out each user from the program and data of all other (unauthorized) users. In addition, a user must not be allowed to interfere with the time-sharing monitor by improper use of input/output commands, halt commands, etc. The latter capability is generally obtained by denying the user certain "privileged" instructions, which may be executed only by "privileged" programs, such as the operating system.

The former is generally provided by memory protection schemes such as relocation and bounds registers [14], segmentation [12, 31], paging [51], and memory keys which allow limited (e.g. read-only) access [32].

All these access control methods protect contiguous portions of (real or virtual) computer memory from alteration by an errant program. They do not, however, provide protection of a user file from unauthorized access. Toward this end, software schemes have augmented the hardware schemes described above.

Methods which enhance data privacy. With respect to the methods which enhance the privacy of data in a shared system, Paul Baran observed in 1966 [5] that "It is a very poorly studied problem.. There is practically nothing to be found in the computer literature on the subject." Since then, awareness has grown, largely as a result of Congressional interest [56, 57]. An entire session of the AFIPS 1967 Spring Joint Computer Conference was devoted to this issue. But only very recently has there been developed a working system with more than password protection at the file level [29].

In nearly all systems to date, a user's password (see Figure 1) will get him into his file directory and into any file referenced in that directory. The most elaborate scheme so far is that of Daley and Neumann [16], which features directories nested to any level used in conjunction with passwords. Each file has access control information associated with itself. Unless one has the "key" to a file, one cannot get at the information in that file. Password schemes permit a small finite number of specific types of access to files, although Daley and Neumann [16] effectively provide more flexible control via a type which allows a user-written program to decide whether each requested access to a file is allowed.

Limitations of these methods. The meth-

STANDARD METHOD

```
LOGIN,MAN2793,ACCTS-17-2.
     PASSWORD?

PRIVACY3.
     FILE NAME?
```

BETTER METHOD WITH THREAT MONITORING

```
LOGIN,MAN2793,ACCTS-17-2.                 10 14 06   TERMINAL 5, 2754, 5-17-2, LOGIN

     PASSWORD(5742)=?
45273.                                    ********
                                          10.14 53   TERMINAL 5, 45273 FAILS ON FILE PASSWORD
     TRY AGAIN.  PASSWORD(9360)=?         ********
69032.                                    10.15 44   TERMINAL 5, 69032 PASSWORD OK
     FILE NAME?
PRIVACY.                                  10.16 35   TERMINAL 5, FILE --PRIVACY-- FILE

     OPERATION?
SORT RECORDS BY DATE.                     10 18.20   TERMINAL 5, SORT RECORDS BY DATE
```

FIG. 1. Password use

ods above necessary for properly operating a time-sharing system perform their task acceptably—they guarantee system integrity. However, the password methods fall short of providing adequate software protection for sensitive files. Password schemes can be compromised by wiretapping or electromagnetic pickup, to say nothing of examining a console typewriter ribbon. Moreover, in some systems the work factor, or cost, associated with trying different passwords until the right one is found is so small that it is worthwhile for an interested but unauthorized user to do just that. Centralized systems tend to have relatively low work factors, since breaking a code in a centralized system generally allows access to more information than in a decentralized system. Some methods used to raise the work factor back to at least the level of a decentralized system are given below.

There is an even more serious problem with password systems. In most current systems, information is protected at the file level only—it has been tacitly assumed that all data within a file was of the same sensitivity. The real world does not conform to these assumptions. Information from various sources is constantly coming into common data pools, where it can be used by all persons with access to that pool. The problem of what to do when certain information in a file should be available to some but not all legal users of the file is not well studied. In the Multics system [12], for example, it is currently the case that if a user has a file which in part contains sensitive data, he just cannot merge *all* his data with that of his colleagues. He must separate the sensitive data and save that in a separate file; the common pool of data does not contain this sensitive and possibly highly valuable data. Moreover, he and those he allows to access this sensitive data must, if they also want to make use of the non-sensitive data, create a distinct merged file, thus duplicating information kept in the system; if some of this duplicated data must later be changed, it must be changed in all files, instead of only one (see Figure 2). If there was a method for placing data with varying degrees of sensitivity into common files such that suitable access control over each piece of data was guaranteed, all the data could be aggregated and processed much more easily. Indeed, many social scientists are in favor of a national data bank for this very reason [8, 20]. On the other hand, precisely because the problem has not been solved

satisfactorily, lawyers [22, 48] scientists [5, 11, 19, 28, 54], urban planners [65], and the general public [53, 55, 63] have become concerned about such a system.

In a recent thesis, Hsiao [29] has suggested and implemented files which contain "authority items"; these authority items control access to records in files. Other proposals which treat access control as a function of the user rather than the data have been advanced by Evans and LeClerc [66] and by Bingham [64]. Hsiao's scheme, however, is the first *working* system which controls access at a level lower than the file level. The implementation depends on a multilist [46] file structure, but the concept of an authority item associated with each user is independent of the structure of the file. The accessibility of a record depends on whether the file owner has allowed access to the requester. This information is carried in the authority item. Capabilities [18] (such as read only, read and write, write only) appear to reside with the file rather than with each record.

A problem with Hsiao's scheme is the duplication in *each pertinent* authority item of entries for protected fields of *one* file. If there are J users of the system and each has K private fields in each of L files, and if each user has access to the files of S other users, then $S \times K \times L$ entries must be made in *each* authority item for user protection. Since there are J users, $T = J \times S \times K \times L$ entries must be maintained in the authority items by the system. For the not unlikely case $J = 200$, $K = 3$, $L = 2$, $S = 10$, we calculate $T = 12{,}000$. Depending on the amount of storage used per entry, this price in storage and maintenance may prove too much to pay in many instances. As S approaches $J - 1$, not only does this price become higher but the system also becomes inefficient (since it maintains lists of *authorized* rather than *unauthorized* file users). Of course, if $S = J - 1$, the entire protection system is unnecessary.

Some other methods for access control have been proposed. Graham [27] has suggested a technique involving concentric "rings" of protection which may prove a reasonable way to provide flexible but controlled access by a number of different users to shared data and procedures. Dennis and Van Horn [18] have proposed that higher-level programs grant access privileges to lower-level programs by passing them "capability lists."

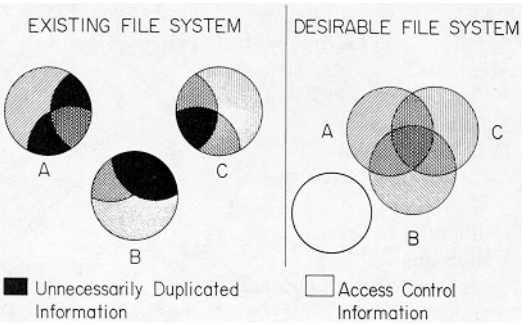

FIG. 2. Use of computer storage in file systems

Graham's scheme has several disadvantages. It assumes a computer with demand hardware segmentation; since, in the opinion of the author, no large computer systems (of the type that would be necessary for a public utility) with these hardware facilities are as yet serving a large user community in an acceptable manner, this assumption may be premature, particularly in light of the alternatives, such as monoprogramming systems which use extended core storage bulk memories [30, 37]. The Graham scheme effectively rules out the use of one-level memories such as associative memories [25], Lesser memories [35], etc., given the current hardware state-of-the-art. If the data bank has many different data fields with many different levels of access, the swap times necessary to access each datum in its own (two-word or so) segment will rapidly become prohibitive using today's technology. In addition, the Graham scheme imposes a hierarchy on all information in the data base; this is not desirable in every instance. The scheme of Dennis and Van Horn suffers from all the drawbacks of the Graham scheme except the last. Com-

TABLE I. SOME THREATS TO INFORMATION PRIVACY
(Extracted from [44])

Accidental
User error
System error
Deliberate, passive
Electromagnetic pick-up
Wiretapping
Deliberate, active
Browsing
Masquerading as another user
"Between lines" entry while user is inactive but on channel
"Piggy back" entry by interception and transmitting an "error" message to the user
Core dumping to get residual information

pensating for this relative simplicity in the control structure, however, is the fact that a very large number of their meta-instructions must be executed for each attempt to access data which is not in a file open to every user.

Some Proposed Safeguards for the Privacy of Information in Files

We now discuss countermeasures that have been proposed to more adequately insure against unauthorized access to information in files. Petersen and Turn have published an excellent paper [44] on the threats to information privacy, and much of the material of this section has been drawn from that paper.

The most important threats to information privacy are shown in Table I. We can counter these threats by a number of techniques and procedures. Petersen and Turn have organized the various countermeasures into several classes: access management, privacy transformations, threat monitoring, and processing restrictions. They have one other class, integrity management (of hardware, software, and personnel), which is not discussed here.

Access management. These techniques attempt to prevent unauthorized users from gaining access to files. Historically, passwords have been almost synonymous with access management. Passwords alone, however, are not enough, as shown above. The real issue in access management is *authentication* of a user's identification. Peters [43] has suggested using one-time passwords: lists of randomly selected passwords would be stored in the computer and maintained at the terminal or kept by the user. "After signing in, the user takes the next work (sic) on the list, transmits it to the processor and then crosses it off. The processor compares the received password with the next word in its own list and permits access only when the two agree. Such password lists could be stored in the terminal on punched paper tape, generated internally by special circuits, or printed on a strip of paper. The latter could be kept in a secure housing with only a single password visible. A special key lock would be used to advance the list." [44] Another method, based on random-number generation, has been suggested by Baran [3].

A novel idea based on the same principle—the high work factor [3] associated with breaking encoded messages appearing as pseudorandom or random number strings [52]—has been suggested by Les Earnest [23]. He proposes that the user log in and identify himself, whereupon the computer supplies a pseudorandom number to the user (see Figure 1). The user performs some (simple) mental transformation T on the number and sends the result of that transformation to the computer. The computer then performs the (presumably) same transformation, using an algorithm previously stored in (effective) execute-only memory at file creation time. In this way, while the user has performed T on x to yield $y = T(x)$, any "enemy" tapping a line, even if the information is sent in the clear, sees only x and y. Even simple T's, e.g.

$$T(x) = \left[\left(\sum_{i \text{ odd}} \text{digit } i \text{ of } x\right)^{3/2}\right] + (\text{hour of the day}),$$

are almost impossible to figure out, and the "cost per unit dirt" [2] is, hopefully, much too high for the enemy. Petersen and Turn point out that one-time passwords are not adequate against more sophisticated "between lines" entries by

infiltrators who attach a terminal to the legitimate user's line. "Here the infiltrator can use his terminal to enter the system between communications from the legitimate user." [44] As a solution, they suggest one-time passwords applied to messages (as opposed to sessions), implemented by hardware in the terminal and possibly in the central processor. This solution may, however, be too costly for most applications. Also, placing access control at the datum level, rather than at the file level, would eliminate many (though not all) problems associated with this type of infiltration.

Babcock [1] mentions a "dial-up and call-back" system for very sensitive files. When a sensitive file is opened by the program of a user who is connected to the computer via telephone line A, a message is sent to the user asking him to telephone the password of that file to the operator over a different telephone line B. The legal user can alter the password at will by informing the data center.

Privacy transformations. Privacy transformations are reversible encodings of data used to conceal information. They are useful for protecting against wiretapping, monitoring of electromagnetic radiation from terminals, "piggy back" infiltration (see Table II), and unauthorized access to data in removable files. Substitution (of one character string for another), transposition (rearrangement of the ordering of characters in a message), and addition (algebraically combining message characters with "key" characters to form encoded messages) are three major types of privacy transformations, which can be (and are) combined to increase the work factor necessary to break a code. This work factor depends (among others) on the following criteria [52]:

1. Length of the key. Keys require storage space, must be protected, have to be communicated to remote locations and entered into the system, and may even require memorization. Though generally a short key length seems desirable, better protection can be obtained by using a key as long as the message itself.

2. Size of the key space. The number of different privacy transformations available should be as large as possible to discourage trial-and-error approaches, as well as to permit the assignment of unique keys to large numbers of users and changing of keys at frequent intervals.

3. Complexity. The cost of implementation of the privacy system is affected by requiring more hardware or processing time, but the work factor may also be improved.

4. Error sensitivity. The effect of transmission errors or processor malfunctioning may make decoding impossible.

Other criteria are, of course, the cost of implementation and the processing time requirements which depend, in part, on whether the communication channel or the files of the system are involved.

More detailed information on uses of privacy transformations is given in Petersen and Turn [44]. A good unclassified discussion of encrypting and cryptanalysis methods, with particular attention paid to "distributed" communication networks (many terminals, many message switching centers, etc.) has been written by Baran [3]. He also has suggested [2] that we should always make use of minimal privacy transformations in the storage and transmission of sensitive data.

Privacy transformations can be performed by appropriate software in terminals and central processors. When desirable, hardware can be used instead. One current system, for example, uses basically a transposition method and is handled with preset plastic scrambler wheels; changes of these wheels are accomplished by time coordination [39].

Threat Monitoring. Petersen and Turn give a good description of threat monitoring [44]: "Threat monitoring concerns detection of attempted or actual penetrations of the system or files either to provide a real-time response (e.g. invoking job cancellation, or starting tracing procedures) or to permit *post facto* analysis. Threat monitoring (see Figure 1) may include the recording of all rejected attempts to enter

the system or specific files, use of illegal access procedures, unusual activity involving a certain file, attempts to write into protected files, attempts to perform restricted operations such as copying files, excessively long periods of use, etc. Periodic reports to users on file activity may reveal possible misuse or tampering, and prompt stepped-up auditing along with a possible real-time response."

Threat monitoring also will help improve the efficiency of the system by reporting widespread use of particular system facilities. These system facilities can be

TABLE II SUMMARY OF COUNTERMEASURES TO THREATS TO INFORMATION PRIVACY (extracted from [44])

Countermeasure / Threat	Privacy Transformations	Threat Monitoring (audits, logs)
Accidental:		
User error	No protection if depend on password; otherwise good protection	Identifies the "accident prone"; provides post facto knowledge of possible loss
System error	Good protection in case of communication system switching errors	May help in diagnosis or provide post facto knowledge
Deliberate, passive:		
Electromagnetic pick-up	Reduces susceptibility; work factor determines the amount of protection	No protection
Wiretapping	Reduces susceptibility; work factor determines the amount of protection	No protection
Deliberate, active:		
"Browsing"	Good protection	Identifies unsuccessful attempts; may provide post facto knowledge or operate real-time alarms
"Masquerading"	No protection if depends on password; otherwise, sufficient	Identifies unsuccessful attempts; may provide post facto knowledge or operate real-time alarms
"Between lines" entry	Good protection if privacy transformations changed in less time than required by work factor	Post facto analysis of activity may provide knowledge of possible loss
"Piggy back" entry	Good protection if privacy transformations changed in less time than required by work factor	Post facto analysis of activity may provide knowledge of possible loss
Entry by system personnel	Work factor, unless depend on password and masquerading is successful	Post facto analysis of activity may provide knowledge of possible loss
Entry via "trap doors"	Work factor, unless access to keys obtained	Possible alarms, post facto analysis
Core dumping to get residual information	No protection unless encoded processing feasible	Possible alarms, post facto analysis
Physical acquisition of removable files	Work factor, unless access to keys obtained	Post facto knowledge form (sic) audit of personnel movements

"tuned," or, if need be, the facilities can be altered to eliminate bottlenecks. If some security restriction is unduly interfering with system operation, threat monitoring should help pinpoint the offending restriction.

Processing restrictions. In addition to the normal memory protection features mentioned in the first part of this section, some processing restrictions may be desirable. Suggestions have included the mounting of removable files on drives with disabled circuits which must be authenticated before access [44], erasure of core

TABLE II *Continued*

Threat \ Countermeasure	Access Control (password, authentication, authorization)	Processing Restrictions (storage, protected privileged operations)
Accidental:		
User error	Good protection, unless the error produces correct password	Reduce susceptibility
System error	Good protection, unless bypassed due to error	Reduce susceptibility
Deliberate, passive:		
Electromagnetic pick-up	No protection	No protection
Wiretapping	No protection	No protection
Deliberate, active:		
"Browsing"	Good protection (may make masquerading necessary)	Reduces ease to obtain desired information
"Masquerading"	Must know authenticating passwords (work factor to obtain these)	Reduces ease to obtain desired information
"Between lines" entry	No protection unless used for every message	Limits the infiltrator to the same potential as the user whose line he shares
"Piggy back" entry	No protection but reverse (processor-to-user) authentication may help	Limits the infiltrator to the same potential as the user whose line he shares
Entry by system personnel	May have to masquerade	Reduces ease of obtaining desired information
Entry via "trap doors"	No protection	Probably no protection
Core dumping to get residual information	No protection	Erase private core areas at swapping time
Physical acquisition of removable files	Not applicable	Not applicable

memories after swapping a program and its data out to an auxiliary storage device, and built-in hardware codes which peripheral devices would transmit to other system components when necessary. Software which limits access rights by terminal is already part of several systems [69].

There is a real question as to what price one is willing to pay for a given amount of privacy [61]. In some instances, one might desire a whole processor to implement the entire file control and privacy system [44]. Most users, however, will probably settle for less privacy at less cost. This has been the experience so far of Allen-Babcock Corporation—they have not implemented their "dial-up and call-back" privacy technique, since none of their customers has demanded it.

Petersen and Turn have summarized their countermeasures to threats against information integrity, and the major part of the table they present is reproduced in Table II.

PROMISING RESEARCH PROBLEMS

In this section we briefly outline some technical problems which offer promising avenues for research in the future. We raise relevant questions, but no answers are proposed in this paper.

For reasons mentioned in the section on the limitations of proposed protection methods, the methods of protection which effectively pass privileges from one program to another are unsatisfactory. We also saw there that protecting data by associating controls with the data at the file level only is not sufficient. What is needed is some means of controlling access to each individual datum. Such a means should (1) be efficient, and (2) not unduly penalize the user who only wants a small part of his file protected. The mechanism may reside in program, data, indexes into an inverted file, authority items [29], or elsewhere.

Several types of controls have been proposed to insure privacy: threat monitoring, privacy transformations, access management, etc. Some hardware countermeasures, such as physical keys which record the key number on a file or output device, have also been suggested. Unfortunately, no systems, hardware or software, simulated or actual, have been built which enable us to evaluate the various costs of processing time, storage space, etc., of these methods. There is almost a complete absence of implementation of nearly all the proposed techniques. Consider, for example, just one of these techniques, privacy transformations. Petersen and Turn [44] discuss the further work that is needed: "Special attention must be devoted to establishing the economic and operational practicality of privacy transformations: determining applicable classes of transformations and establishing their work factors; designing economical devices for encoding and decoding; considering the effects of query langauge structure on work factors of privacy transformation; and determining their effects on processing time and storage requirements."

The implementation of a (real or simulated) system which uses many countermeasure techniques would be a very desirable undertaking. It would enable us to evaluate the effectiveness and the costs of each technique. A suitably designed system would at the same time allow us to vary the structure of a file. Since the structure of a file may affect quite strongly the access control method used, a number of interesting experiments could be performed. For example, one might consider physically separating the more sensitive data in a hierarchical tree-structured file from the less sensitive data. The more sensitive data could be stored in a memory which was logically at a low level and physically removed from higher-level data. This solution would not be feasible in certain types of associative memories, since the control would require all data to be at the same level.

As another example, the existence of indexes into a tree-structured file (i.e. the use of an inverted file) might strongly alter the operating characteristics of the

access control mechanism by allowing control information to reside in the indexes rather than (say) with the data itself. Further investigation of this relationship is also warranted.

SUMMARY

It is hoped that this paper may help increase awareness of the computer privacy problem and the need for further investigation. Paul Baran puts it well [2]:

"What a wonderful opportunity awaits the computer engineer to exercise a new form of social responsibility. The advent of the new computer-communications technology need not be feared with trepidation as we approach 1984. Rather, we have in our power a force which, if properly tamed, can aid, not hinder, raising our personal right of privacy.

"If we fail to exercise this unsought power that we computer engineers alone hold, the word 'people' may become less a description of individual human beings living in an open society and more a mere collective noun.

"It may seem a paradox, but an open society dictates a right-to-privacy among its members, and we will have thrust upon us much of the responsibility of preserving this right."

ACKNOWLEDGMENTS

The author wishes to thank Professor William F. Miller and Mr. John V. Levy for their encouragement during the preparation of this paper.

BIBLIOGRAPHY

1. Babcock, J. D. A brief description of privacy measures in the RUSH time-sharing system. Proc. AFIPS 1967 Spring Joint Comput. Conf., Vol. 30, Thompson Book Co., Washington, D. C., pp. 301–302.

   A brief summary of the file security procedures in RUSH. This article contains some good but short discussion of possible threats and countermeasures.

2 Baran, P. Communications, computers and people. AFIPS 1965 Fall Joint Comput. Conf Vol. 27, Pt. 2, Thompson Book Co., Washington. D. C., pp. 45–49.

   A well-thought-out general discussion of the privacy problem which overlaps somewhat with Baran's testimony before the Gallagher subcommittee (see [56]). Some specific proposals are presented to deal with the problem.

3 Baran, P. On distributed communications. IX. Security, secrecy and tamper-free considerations. Doc. RM-3765-PR, Rand Corp., Santa Monica, Calif., Aug. 1964.

   A consideration of the security aspects of a distributed communication system, written from the viewpoint that we should fully anticipate the existence of spies within our ostensibly secure communications secrecy protection structure; "Hence, our primary interest should be in raising the 'price' of espied information to a level which becomes excessive." The proposed system combines end-to-end and link-by-link cryptography, automatic error detection and repeat transmission, path changing, and use of a scheme requiring complete and correct reception of *all* previous traffic in a conversation in order to decrypt subsequent message blocks. It assumes enemy infiltration and takes these countermeasures: key bases split over N (> 1) individuals; filtering tests; key change for each conversation; heavy system use for unclassified traffic Contents: I. Introduction; II The Paradox of Secrecy about Secrecy; III Some Fundamentals of Cryptography; IV Implications for the Distributed Network System, V. A "Devil's Advocate" Examination.

   This paper gives a clear, well-written discussion of an often "touchy" subject. Relevant points are brought out by good diagrams. It is one of the clearest expositions of real-life problems and solutions to be found in the open literature

4. Baran, P. Remarks on the question of privacy raised by the automation of mental health records. Doc. P-3523, Rand Corp., Santa Monica, Calif., Apr. 1967.

   Remarks invited for presentation before the American Orthopsychiatric Association Workshop. "The Invasion of Privacy," held in Washington, D. C., 21–23 March 1967. This speech of Baran presents to an intelligent group of computer laymen a view of computer privacy invasion which heretofore has been available only to people in the computer field. Some tales of medical record leaks are recalled. The famous tale of the MIT freshman who programmed the computer to dial simultaneously every telephone extension in the school is retold, thus the importance of "people-proof" systems is graphically illustrated.

   It is a very good paper which can be used to alert intelligent people to the implications of the computer age for privacy.

5. Baran, P. Statement in [56], pp. 119–135.

6. Bauer, K. G. Progress report to U. S. Public Health Service on contract PH 110-234 Joint

Center for Urban Studies of MIT and Harvard, Cambridge, Mass., Jan. 1968. (Mimeographed)

The report contains a nine-page section on the privacy issue as it relates to a proposed health information system for the Boston area. "... Right now our project has a unique opportunity to propose safeguards to privacy in the design of an information system at a time when the crucial operational decisions have not yet been made...." The section discusses present safeguards to record disclosure Currently, privacy is not really insured, and only the excessive cost of getting sensitive information (because of the unwieldiness of current noncomputerized systems) prevents almost all unauthorized access. "... With proper safeguards computerization makes such information far easier to guard..."—why this is the case is explained. A broad framework of new safeguards, combining legal, technological, and administrative measures is being urged, and these are gone into very briefly, with references to a few papers The committee hopes during the coming months to define levels of security and to suggest specific access rules and rights of patients that should be kept in mind.

7 BERKELEY, E. C. Individual privacy and central computerized files. *Comput. Automat. 15*,10 (Oct. 1966), 7.

This article discusses a privacy bill of rights initially suggested by Professor John McCarthy in [38].

8. BOWMAN, R. T. Statement in [56].

9. BRICTSON, R. C. Computers and privacy—implications of a management tool Doc. SP-2953/001/00, System Development Corp., Santa Monica, Calif., 14 Mar. 1968.

10. BRICTSON, R. C. Some thoughts on the social implications of computers and privacy. Doc. SP-2953, System Development Corp., Santa Monica, Calif., 25 Sept 1967.

This is a reprint of a talk presented to the American Society for Industrial Security as part of a panel, "Problems in the Age of the Computer," 13th annual seminar, 12–14 September 1967, Los Angeles, California. Briefly discussed are (1) the computer as an innovation and tool, along with some of the anxieties it creates, (2) a framework for an inquiry into the problem, (3) responsibilities of organizations and the establishment, (4) socialization—the preparation of new members for entry into society, (5) some examples reflecting issues, and (6) possible remedies. In eleven short pages a quite readable discussion, understandable to the lay person, is given. The framework suggested for investigation seems quite reasonable, and represents one of the few attempts to define the general problem before rushing off to tackle it. This structure considers information from the standpoint of (1) acquisition; (2) access; (3) dissemination; (4) retention; (5) revision, including updating, rejoinder and redress, (6) destruction; and (7) time cycles. Brief examples are given for acquisition and protection. A good case (and a brief one) for the existence of professional ethics codes is made, much better than the discussion in [41] by Parker. Five guidelines for public policy makers are suggested: (1) specifications of benefits; (2) catalogue of potential risks; (3) directory of preventive safeguards and controls; (4) inventory of antidotes and countermeasures, (5) index of penalities and sanctions.

A very good paper for the layman and interested computer scientist.

11. CALDWELL, L. K. (Ed.) *Science, Technology, and Public Policy—A Selected and Annotated Bibliography (Volume 1)*. Dep. of Government, Indiana U., Bloomington, Ind., 1968, pp. 207–210.

Pages 207–210 comprise Section 6.4, "Privacy," and contain an annotated bibliography of 13 entries. [40] and [22] are included, and [62] is based on two other entries in the bibliography. The others deal with privacy as an aspect of human dignity, lie detectors, wiretapping, concepts of consent and confidentiality, and eavesdropping. The entire bibliography should be useful to students of sociology Its sections are.

1. Bibliographies and Research Tools
2. Philosophy of Science
3 History of Science and Technology
4. Nature and Impact of Science and Technology
5. Science, Politics, and Government
6. Science, Technology, and the Law
7. Science, Education, and the Universities
8. Scientific and Technical Personnel
9 Scientific Organizations and Institutions
10. Organization and Management of Research and Development
11. Science, the Humanities, and Religion
12. Science and Society

12. CORBATO, F. J., AND VYSSOTSKY, V. A. Introduction and overview of the Multics system. Proc. AFIPS 1965 Fall Joint Comput. Conf., Vol. 27, Pt. 1, Spartan Books, New York, pp 185–196.

13 Computer Research Corp. Time-sharing system scorecard, No. 5. Computer Research Corp., Newton, Mass , 1967.

14 Control Data Corp. Control Data 6400/6600 computer systems reference manual. Pub. No. 60100000, Control Data Corp., St. Paul, Minn., 1966.

15. CRISMAN, P. A. (Ed.). *The Compatible Time-Sharing System—A Programmer's Guide* (Second ed.). MIT Press, Cambridge, Mass., 1965.

16. DALEY, R. C., AND NEUMANN, P. G. A general-purpose file system for secondary storage. Proc. AFIPS 1965 Fall Joint Comput. Conf., Vol. 27, Pt.1, Spartan Books, New York, pp. 213–229.

This system places access control on the branches of a tree-structured file directory. Five modes of control are allowed—trap, read, execute, write, and append. The paper contains some of the best thinking yet about a practical, general solution to lower-level access control. One of the "Multics papers," this is must reading for data base system designers.

17. DAVIES, L. E Computer plan for personal

"dossiers" in Santa Clara stirs fears of invasion of privacy. *The New York Times*, 1 Aug 1966, p. 27.

18. DENNIS, J. B., AND VAN HORN, E. C. Programming semantics for multiprogrammed computations *Comm ACM 9*,3 (Mar 1966), 143–155

A number of meta-instructions are defined which relate to programming operations in multiprogrammed systems These are related to parallel programming, protection of separate computations, sharing of files, and memory. Some very good and long-neglected ideas are set forth here. Capabilities of a computation are related to segments. In practice, capabilities should be related to some smaller basic units, e.g. nodes of a tree

19 DEUTSCH, L P Snooping by computer (letter to the editor). *San Francisco Chronicle*, 19 July 1968

A computer scientist experienced in time-sharing systems warns against misuse of computers In particular, he laments the lack of adequate protection in the California Department of Social Welfare data bank

20. DUNN, E. S., JR. Statement in [56], pp 92–95

21. DUNN, E S, JR. The idea of a national data center and the issue of personal privacy *Amer Statis 21* (Feb. 1967), 21–27

An attempt by the author of the Bureau of the Budget report which recommended the establishment of a national data center to correct "certain obvious misinterpretations and set forth more explicitly some views on the very important issue of personal privacy." He maintains that we can immediately begin to save much "harmless" data in a "statistical" data bank and that we have 10 or 15 years to figure out how to protect privacy The trade-offs for and against some sort of national data bank are more clearly delineated than in the original report

22 Duke University School of Law. Privacy. *Law and Contemporary Problems 31,* 2 (Spring 1966), 251–435

This is an entire issue of *Law and Contemporary Problems* devoted to privacy. Its contents are: Clark C. Havighurst, "Foreword"; William M. Beany, "The Right to Privacy and American Law", Milton R Konvitz, "Privacy and the Law: A Philosophical Prelude"; Edward Shils, "Privacy Its Constitution and Vicissitudes"; Sidney M Jourard, "Some Psychological Aspects of Privacy"; Glenn Negley, "Philosophical Views on the Value of Privacy"; Harry Kalven, Jr., "Privacy in Tort Law—Were Warren and Brandeis Wrong?"; Kenneth L Karst, "'The Files'. Legal Controls Over the Accuracy and Accessibility of Stored Personal Data", Joel F. Handler and Margaret K. Rosenheim, "Public Assistance and Juvenile Justice", William A Creech, "The Privacy of Government Employees."

The issue contains nothing on computers except in the Karst paper, which has about four pages on the effect of automation. The possible solutions to this aspect of the privacy problem are dealt with in superficial detail, but relevant references are given for the reader interested in a more advanced technical discussion

23. EARNEST, L. Private communication.

24 ERVIN, S. J. The computer—individual privacy. *Vital Speeches of the Day 33*, 14 (1 May 1967), 421–426

Senator Ervin discusses the impact of the computer on national life in a speech to the American Management Association. He thinks that in order to avoid strict legislative controls and the denial of government research and development funds, the industry must devise safeguards against improper data access, illegal tapping, and purloined data in shared systems. He likes the idea of an industry ethical code.

25. FELDMAN, J A. Aspects of associative processing. Tech. Note 1965-13, Lincoln Laboratory, MIT, Cambridge, Mass., 1965

26 GALLATI, R. R. J. The New York State identification and intelligence system. In [56], pp. 159–168.

27 GRAHAM, R. M. Protection in an information processing utility. *Comm. ACM 11*, 5 (May 1968), 365–369.

A good five-page paper on the topic A solution to the file access problem is given which involves rings or spheres of protection for both data and programs (in particular, for segments, as at Project MAC). The main drawbacks are (1) the method is tied to segments, which in practice are fairly large blocks of memory, protection of a smaller area wastes the rest of the segment; and (2) parallel processes or processors may render parameters or data invalid if proper safeguards are not taken. If these problems are solved, this method provides flexible but controlled access by a number of different users to shared data and procedures

28 HARRISON, A. The problem of privacy in the computer age: an annotated bibliography Doc RM-5495-PR/RC, Rand Corp., Santa Monica, Calif., Dec. 1967.

This is a must document. This 300-entry bibliography is well-annotated and indexed by author as well as by each of the following categories. cashless-checkless society, time-sharing, data banks, media, social scientists' views, bill of rights, electronic eavesdropping and wiretapping, computer utilities, Congressional view of privacy, legal views, system security, technologists' views.

29 HSIAO, D. K *A File System for a Problem Solving Facility.* Ph.D. Diss. in Electrical Engineering, U. of Pennsylvania, Philadelphia, Pa., 1968.

An important new concept is introduced and implemented on the file system at Penn. This concept, that of the authority item, allows control within files over data access. Each field in a file can be protected from unauthorized access. Data records need not be reprocessed if a change in a record's protection status or in a user's level of accessibility occurs The capability to read only, write only,

etc., goes with an authority item and not with a record. Protected records are completely nonexistent as far as the unauthorized user is concerned. The system as currently implemented is dependent on the file structure (multilists). However, the idea of authority items is not and is an important new concept. This thesis should be examined by those who have the responsibility for access control in their own file systems. It appears to be the first working system with protection below the file level.

30. HUMPHREY, T. A. Large core storage utilization in theory and in practice. Proc. AFIPS 1967 Spring Joint Comput. Conf., Vol. 30, Thompson Book Co., Washington, D.C, pp. 719–727.

31. IBM System/360 Model 67 functional characteristics. Form A27-2719-0, IBM Corp., Kingston, N. Y., 1967.

32. IBM System/360 principles of operation. Form A22-6821-2, IBM Corp., Poughkeepsie, N. Y., 1966.

33. JANSSEN, R F. Administration studies plan to generalize data, hopes to avoid "police state" image. *Wall Street J.*, 11 Nov 1966, p. 6.

34. KAYSEN, C. Data banks and dossiers. *The Public Interest* (Spring 1967), also in [57], p. 265.

The case "for" a national data bank, in the light of the mauling this proposal got before the Gallagher subcommittee.

35. LESSER, V. R. A multi-level computer organization designed to separate data-accessing from the computation. Tech. Rep. CS90, Comput. Sci. Dep., Stanford U., Stanford, Calif., 11 Mar. 1968.

36. LICKSON, C. P. The right of privacy in the computer age. *IEEE Comput. Group News 2*, 1 (Jan. 1968), 13–17.

A nontechnical five-page paper which defines privacy, examines some historical court cases dealing with it, and tries to pinpoint current legislative trends in this area. "... Legislation and court decisions can catch up to the state of the art." A good general overview from a nontechnical standpoint, the article is well-referenced.

37. MACDOUGALL, M. H. Simulation of an ECS-based operating system. Proc AFIPS 1967 Spring Joint Comput. Conf., Vol. 30, Thompson Book Co , Washington, D C., pp. 735–741.

38. MCCARTHY, J. Information. *Sci Amer. 215*, 3 (Sept. 1966), 64–73.

McCarthy, in a very good survey article on computation, proposes a computer bill of rights which would help to guarantee privacy in computer-based data files

39. MCLAUGHLIN, F. X. Private communication.

40. MICHAEL, D. N. Speculations on the relation of the computer to individual freedom and the right to privacy. *George Washington Law Rev. 33*(1964–65), 270–286.

Between now and 1984, business and government will use extraordinary advances in computer technology to file and collate "personal" facts about private citizens and even to telemeter the populace. What are the implications for traditional ideas of freedom and privacy? Will such progress be met with constitutional objections or with public acquiescence?—Author's Abstract

This well-written nontechnical paper makes some valid and oft-overlooked points. It outlines factors which, in the past, have made privacy invasion difficult (1) data available but uncollected and uncollated, (2) data not recorded with precision and variety necessary to gain new or deeper insight into the private person, (3) difficulty of keeping track of a particular person in a large and highly mobile population; (4) difficulty of access to already filed data about the private person; (5) difficulty of detecting and interpreting potentially self-revealing private information within available data.

Points for a central data bank are validly and tellingly made, and the point is made that now, as in the past, people may give up some freedom to protect or enhance another freedom. Ways in which corruptible programmers may become privy quite legally to privileged information are discussed. A short and worthwhile paper.

41. PARKER, D. B. Rules of ethics in information processing. *Comm. ACM 11*,3 (Mar. 1968), 198–201.

42. PARKER, R. W. The SABRE system. *Datamation 11*, 9 (Sept. 1965), 49–52.

43. PETERS, B. Security considerations in a multiprogrammed computer system. Proc. AFIPS 1967 Spring Joint Comput. Conf., Vol. 30, Thompson Book Co., Washington, D.C., pp. 283–286.

A specific list of desirable and necessary security safeguards for file systems is given. Hardware, software, and administrative safeguards are discussed

44. PETERSEN, H. E., AND TURN, R. System implications of information privacy. Proc. AFIPS 1967 Spring Joint Comput. Conf, Vol. 30, Thompson Book Co., Washington, D.C., pp. 291–300. (Also available as Doc. P-3504, Rand Corp., Santa Monica, Calif., Apr. 1967.)

"Various questions of providing information privacy for remotely accessible on-line, time-shared information systems are explored.... A range of protective countermeasures is discussed, and their choice and implication considered. It appears possible to counter a given level of threat without unreasonable expenditures of resources. The protective techniques discussed ... include: shielding to reduce electromagnetic emanations; use of once-only passwords for access control; application of privacy transformations to conceal information in user-processor communications and in data files; recording of attempted penetrations; and systematic verification of the hardware and software integrity."—Authors' abstract

This is must reading. It contains a detailed and well-written discussion of threats to file security and countermeasures against these

threats. In particular, problems at the processor, the files, the terminals, and the communication lines are discussed. A good bibliography is given.

45. PROSSER, W. L. Privacy. *California Law Rev. 48*,3 (Aug. 1960), 383–423.

A review of court cases dealing with a "right to privacy." The review appears to be comprehensive (to this layman at law). The author, then Dean of the University of California Law School at Berkeley, contends that four distinct kinds of privacy invasion cases can be described: (1) intrusion upon seclusion or solitude, or into private affairs; (2) public disclosure of embarrassing private facts; (3) publicity which places the plaintiff in a false light in the public eye, (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness. The article is well-written and interesting. As a final fillip, I can not conclude without praising the author for making me aware of "a possible nomination for the all-time prize law review title, in the note 'Criminination of Peeping Toms and Other Men of Vision,' *Ark Law Rev. 5*(1951), 388."

46. PRYWES, N. S. A storage retrieval system for real-time problem solving. Rep. No. 66-05, U. of Pennsylvania Moore School of Electrical Engineering, Philadelphia, Pa., 1966.

47. RAMEY, J. W. Computer information sharing—threat to individual freedom. Proc. of the Amer. Documentation Institute, 1967, pp. 273–277.

This paper discusses, for a lay audience, why centralized data banks threaten privacy. It proposes licensing of computer professionals, much as CPA's are licensed now. It also proposes legislation to allow an individual to inspect his entire dossier, delete inaccuracies via court order, and prohibit transfer of information identifiable with himself to a linked data bank without his express consent.

48. REICH, C. A. Statement in [56].

49. SCHWARTZ, J. I. The SDC time-sharing system. *Datamation 10*,11 (Nov. 1964), 28–31.

50. SCHWARTZ, J. I. The SDC time-sharing system. *Datamation 10*,12 (Dec. 1964), 51–55.

51. Scientific Data Systems. SDS 940 computer reference manual. Pub. No. 90 06 40A, Scientific Data Systems, Santa Monica, Calif., Aug. 1966.

52. SHANNON, C. E. Communication theory of secrecy systems. *Bell Syst. Tech. J. 28*, 4 (Oct. 1949), 656–715.

A mathematical theory of secrecy systems is developed and presented in a most readable form. First, basic mathematical structure of secrecy systems is dealt with. Examples of various types of ciphers are given. Measures of "how secret" a system is are introduced, and it is shown that "perfect" secrecy is possible but requires, if the number of messages is finite, the same number of possible keys. A measure of "noise" in a message is given and strongly ideal systems where this cannot be decreased by the cryptanalyst are discussed. Finally, an analysis of the basic weaknesses of secrecy systems is made. This leads to methods for constructing systems which require a large amount of work to solve. Finally, a certain incompatibility among the various desirable qualities of secrecy systems is discussed. An excellent paper, and doubly so for the nonfainthearted in mathematics (particularly probability and modern algebra).

53. Social workers balk at computers. *San Francisco Chronicle*, 16 July 1968, p. 2.

This newspaper article describes how over 20 state social workers picketed the state department of social welfare in protest over a new departmental regulation requiring them to supply computers with "intimate facts" about the mental illness of their clients. The data was linked to the client's social security number.

54. SQUIRES, B. E., JR. Statement in [56].

55. STAR, J. The computer data bank. will it kill your freedom? *Look* (25 June 1968), 27–29.

A short, very well-written popular survey of computers and privacy. Some well-detailed accounts of uses computer data banks are being put to today are presented.

56. U. S. Congress. The computer and the invasion of privacy—hearings before a subcommittee of the Committee on Government Operations, House of Representatives, 89th Congress, Second Session (Gallagher Report), U. S. Government Printing Office, Washington, D.C., 26–28 July 1966.

Pro and con on a national "statistical" data bank—the full testimony.

57. U. S. Congress. Computer privacy—hearings before the Subcommittee on Administrative Practice and Procedure of the Committee on the Judiciary, United States Senate, 90th Congress, First Session (Long Report), U. S. Government Printing Office, Washington, D.C., 14–15 March 1967.

The full testimony before the Long subcommittee on computer privacy.

58. WARBURTON, P. Letter to the editor. *Comput. Automat. 16*,5 (May 1967), 8.

A "Resolution on the National Data Center and Personal Privacy" proposed by the Washington, D.C. Chapter of the Association for Computing Machinery is given

59. WARE, W. H. Security and privacy in computer systems. Proc. AFIPS 1967 Spring Joint Comput. Conf., Vol. 30, Thompson Book Co., Washington, D.C., pp. 279–282.

This is a general outline of the major vulnerabilities of time-sharing systems which handle sensitive data. It also served as an introductory paper for the session on privacy at the conference.

60. WATSON, T. J., JR. Technology and privacy. Speech given to Commonwealth Club of California, Hotel St. Francis, San Francisco, Calif., 5 Apr. 1968.

An address by the Chairman of the Board of IBM to the Commonwealth Club of California. Watson discusses in general what the privacy problem is, advantages and disad-

vantages of centralized data banks, and possible steps toward solving the problem. Suggestions are given for legal, ethical, and technological safeguards.

61. WEISSMAN, C. Programming protection: what do you want to pay? *SDC Mag. 10*,7–8 (July, Aug. 1967), System Development Corp., Santa Monica, Calif.

62. WESTIN, A. F. *Privacy and Freedom*. Atheneum, New York, 1967.

A comprehensive, well-written book on the relationship of privacy to freedom, tracing "privacy rights" from 1776 to the present. The emphasis is on the present and the future. The book has four parts: (1) the functions of privacy and surveillance in society, (2) new tools for invading privacy, (3) American society's struggle for controls (five case studies), and (4) policy choices for the 1970's. Each part is copiously documented, and in addition there are four bibliographies at the end: the functions of privacy, the new technology, the struggle for controls, and privacy in American law and policy. The section on computer technology and possibilities for it by 1975 is quite enlightening. Numerous legal decisions are cited in this seminal work. It is must reading for those seriously concerned with the general problem of privacy.

63. WESTIN, A. F. The snooping machine. *Playboy 15*, 5 (May 1968), 130ff.

A good review of initial and revised ideas on a national data bank. The advantages and disadvantages are set forth in this article in a nontechnical (!) publication. An interesting account of the automated adventures of a mythical citizen in 1975 is given

64. BINGHAM, HARVEY W. Security techniques for EDP of multilevel classified information. Doc. RADC-TR-65-415, Rome Air Development Center, Griffiss Air Force Base, New York, Dec. 1965. (Unclassified)

The study objective was to develop hardware and software techniques for security (need-to-know) control of on-line users and programmers in multiprogramming, multiprocessing EDP systems of apparent future development. Hardware techniques recommended include: (1) processors having two modes of operation, interrupt entry into control mode in which privileged instructions are executable, flag bits for identification and control of memory words, and address checks against access-differentiated memory bounds; (2) parity checks on intermodule information transfers; (3) input/output control processors, which establish and verify peripheral unit connections, check memory addresses against bounds, and confirm security content of record headers being transferred; and (4) bulk file control of physical record integrity, and lock control over write permission and flag bit setting to permit supervisor establishment of control programs. Software techniques reside in the executive control program and are executed in control mode and identified by flag bits. Security routines are described and evaluated which construct, protect, and check access requests against user security control profiles, verify memory bounds and memory blanking, and provide security indicators for input/output. The integrated techniques are applied to control users and system programmers in an advanced modular system. Retrofit of most of the recommended techniques to an existing data processor (the Burroughs D825 Modular Data Processing System) is feasible. An external retrofit unit is described which provides control mode and privileged instructions for single-mode processors.—Author's Abstract

This paper is the final report of an eight-month study program conducted by the Burroughs Corporation for the US Air Force. It is a highly technical description of a proposed multiprogramming, multiprocessing, on-line computer system designed with security of information in mind. A very detailed report, it deals with technical aspects of a computer system operating in a secure environment; the report does not touch on cryptography, long-distance communications problems, electromagnetic radiation monitoring, physical security, equipment wiretapping or physical modifications, personnel problems, or administrative procedures.

Recommendations made by the study are described in the author's abstract above. In addition the reviewer notes the following which may be of interest. Physical keys associated with a user are recommended (p. 7). The system requires the user (or an operator with a master key) to be physically present at a terminal before input or output can occur. An execute-only bit in each word is recommended (p. 9). This is turned on in routines of the operating system, thus guaranteeing its integrity.

The amount of hardware over and above that required for a traditional system is detailed in terms of "equivalent flip-flops" in Table 2, p. 56. Software security techniques are summarized on pp. 71–72. An attempt is made to gauge the costs of these techniques on pp. 99–100, the units of measurement being additional instruction executions necessary and additional storage space used. Ample justification is not given for these estimates, which tend to be plausible but low. A detailed description of startup procedures for this security-oriented system is given on pp. 77–80. Tables of all hardware and software security techniques which were considered in the study (not only the ones recommended), along with their application, what they protect against, and additional comments, are given on pp. 119–127. Pages 101–112 describe the detailed interfaces recommended for security between terminal units, bulk files, and the input/output control processor. Pages 113–117 detail retrofits (changes) necessary to implement the proposed system on the Burroughs D825 computer system, an existing multiprogramming and multiprocessing system. General flowcharts of key security routines are given in Appendix I. A brief discussion of the literature on error-correcting codes and redundancy techniques is given in Appendix IV. Pages 115 and 116 are switched

in this report of 173+xiii pages, which contains 12 illustrations, tables, and a glossary

This report should definitely be read by all who plan to design or configure a computer system in which secure information must be protected.

65. DUEKER, K. J. Data sharing and confidentiality in urban and regional planning. Proc. Urban Inform. Syst. Assoc. Fifth Annual Conf., Garden City, N.Y., 8 Sept. 1967.

A good overview for statisticians, urban planners, and the interested layman of the computer privacy problem. The first 15 pages present a good summary of the computer invasion of privacy literature. The latter 11 pages present implications of the National Data Center proposal to planners at the state and local levels. The latter part will interest urban planners particularly, while the former is of general interest. This easily readable paper is not at all technical. Some of the references do not exist in the volumes cited.

66. EVANS, D. C., AND LE CLERC, J. Y Address mapping and the control of access in an interactive computer. Proc. AFIPS 1967 Spring Joint Comput. Conf., Vol. 30, Thompson Book Co., Washington, D.C., pp. 23–30.

An idea for extended segmentation hardware is presented. This hardware would control access paths at execution time, permit selective input and output operations under actual control of interactive users, and eliminate the need for relocation of programs at load time. Access control is by hardware at the segment level. The system has not been implemented, although "the hardware and software problems have been analyzed extensively," according to the paper, in the Ph.D. dissertation of the second author. The ideas on access control, whether eventually done in hardware or software, are steps in the right direction.

67. SAWYER, J., AND SCHECHTER, H. Computers, privacy, and the national data center: the responsibility of social scientists *Amer. Psychologist 23*, 11 (Nov. 1968).

A paper for social scientists discussing the advantages to be gained by creation of a national data center and the pitfalls vis-a-vis privacy. The paper gives a good history of the proposal for a national data center and an excellent view of what stage the proposal is in currently (August 1968). It presents an excellent suggestion. namely, that only random samples of respondents be kept (one in 1000 samples are adequate for most analyses in the social sciences).

68. U. S Congress. Privacy and the national data bank concept House Committee on Government Operations, U.S. Government Printing Office, Washington, D.C., 2 Aug. 1968.

A very excellent review of the national data bank concept, which explains why such a system would be most helpful in certain areas and how it poses grave threats to privacy if not carefully designed. Initial actions by the Bureau of the Budget to study the feasibility of a central, computer-based data bank are reviewed very briefly, as are the hearings of the House of Representatives Special Subcommittee on Invasion of Privacy. The Committee on Government Operations notes that "the reports commissioned by the Bureau of the Budget do not contain well-thought-out theoretical or practical procedures necessary to insure privacy" and that the Budget Bureau "has not come to understand fully the importance of privacy in the National Data Center system." It suggests in detail procedures, safeguards, and alternatives to be considered in formulating specific proposals for a national data bank. These can be applied to *any* data base of sensitive information and should be quite carefully considered by designers of any such data bank, public or private. This 34-page document is a gem and an absolute must for those concerned with the specter of a national data bank.

69. Santa Clara (California) County. LOGIC User's Guide for Terminal Inquiry Systems. General Services Agency, Data Processing Center, Santa Clara County, Calif., 1 Aug. 1967.