WORKING PAPER
ALFRED P. SLOAN SCHOOL OF MANAGEMENT

PRIVACY, TECHNOLOGY, AND THE AMERICAN CITIZEN

Stephen J. Williams
Richard Owens
Edouard Cointreau
Peter Bloomsburgh

563-71
October

MASSACHUSETTS
INSTITUTE OF TECHNOLOGY
50 MEMORIAL DRIVE
CAMBRIDGE, MASSACHUSETTS 02139

PRIVACY, TECHNOLOGY, AND THE AMERICAN CITIZEN

Stephen J. Williams
Richard Owens
Edouard Cointreau
Peter Bloomsburgh

563-71
October

PRIVACY, TECHNOLOGY, AND THE AMERICAN CITIZEN

by

Stephen J. Williams
Richard Owens
Edouard Cointreau
Peter Bloomsburgh

Privacy, Technology, and the American Citizen *

1 INTRODUCTION

The right to privacy has been an issue of considerable prominence in recent months as the Congress and the American public have increasingly questioned the extent and nature of the Constitutional and moral ramifications of privacy. This article presents an examination of privacy with particular emphasis on the implications of technological advancement. A framework is developed within which managerial decisions related to questions of privacy can be examined.

An initial investigation of the definition of privacy is presented which distinguishes between the individual's need for privacy and the society's requirements for infringing upon that need. Next, the technological determinants of privacy are examined, including the utilization of advanced electronic equipment (especially the computer) to collect information. The unique properties and problems inherent in multiple-access time-sharing systems are considered.

All of these issues are integrated into a framework for the analysis of specific databanks. This framework may be applied to databanks currently in existence and to those which may be proposed at some future time. The

guidelines presented are intended as an aid in determining the suitability of such databanks.

Finally, a number of proposed solutions to the problems of privacy are examined, followed by suggestions for further thought.

2 PRIVACY: THE PROBLEM

Privacy concerns everyone. Although most Americans would agree that no one should take a challenge to his privacy lightly, few carefully consider the implications of applying for a credit card or a bank loan. Any time a transfer of information occurs, privacy is in some way affected, whether it be our personal privacy, that of our friends or neighbors, or the privacy of an organization. Concurrently with our individual considerations of privacy, we must act as a nation to forge a clear national policy.

Privacy is not easily defined. In fact, there is no widely accepted definition in use today, although at least one excellent definition (in the logical sense) has been presented. In legal terminology, a satisfactory definition remains to be established. (See also (2))

2.1 Definition of Privacy

The most important dimensions of privacy can be seen through an examination of statements made by various individuals who have wrestled with the problem. Arthur Goldberg, former Associate Justice of the United States Supreme Court has put forth the following observation:

> "The dwindling of privacy has been as frequently noted as the rise in crime. In the modern world, we have only belatedly realized that privacy is an increasingly scarce social resource, and one which must be vigilently protected against the claims of efficient social ordering."
> (16)

Congressman Cornelius Gallagher, speaking before the American Management Association, has defined privacy as:

> "...the free choice by a free man in disclosing to public record certain basic facts about his actions, thoughts, and decisions."(12)

He goes on to say:

> "Liberty under law...the cornerstone of a free America...demands that the past be a springboard to the full expression and use of ability and not an anchor which pulls a man down, and drowns him in youthful mistakes or unevaluated early decisions."(12)
> (See also (9),(10),(11),(13))

These attempts at definitions are, however, incomplete. The most comprehensive definition of privacy is offered by Professor Alan F. Westin (See also (20),(21)); it highlights the privacy decision as the choice of the individual in trading off his desire to be an individual, and his desire to participate in society:

> "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.... The individual's desire for privacy is never absolute, since participation in society is an equally powerful desire. Thus each individual is continually engaged in a personal adjustment process...in the face of pressures from the curiosity of others and from the processes of surveillance that every society sets in order to enforce its social norms."(19)

2.2 The Individual's Viewpoint

Several facets of privacy are important from the individual's viewpoint. In his book, Privacy and Freedom (19), Professor Westin has identified four primary functions which privacy performs.

A. Individuals intrinsicly seek personal autonomy. Privacy provides the capability for individuals to control the flow of information that relates to their personal lives, and, by so doing, provides a means for them to direct some aspects of their existence. Indeed, the history of literature is marked by references to controlling one's fate. In an ever more complex and active society, this function of privacy assumes an ever increasing importance.

B. Privacy protects people from undue consequences resulting from the expression of anger and frustration. Through this function, then, individuals are afforded the opportunity for emotional release without the continuous damper that a record of their actions would cause. Of course, when the actions of emotional release infringe upon the rights of others, response by the society is justified.

C. Privacy provides for self evaluation and introspection. Individuals must be allowed to evaluate their own performance for the purpose of determining their desires and actions. Privacy allows this self-supervision without the constant feeling that someone is looking over your shoulder. Again, this function is not absolute -- the

evaluation of an employee by his supervisor, for example, is legitimate.

D. Privacy allows for the protected and privileged transfer of information. Within this context, an individual is granted the opportunity to discuss a supervisor with another employee without fear of dismissal.

But the need for privacy goes even beyond such logical considerations. The work of many anthropologists, sociologists, and biologists indicates strongly that privacy is a biological necessity for human beings. Professor Westin has discussed studies of animal behavior which show that men and animals may very well share basic mechanisms for seeking privacy within their environments. (19) Extrapolating from the great importance ascribed to privacy in the animal world, one must assume that privacy is an even more significant determinant of behavior in the human species. Perhaps the inherent desire in each of us to occasionally seek solitude is an illustration of this need.

2.3 Conflicts of Privacy

However, consideration of the privacy problem on an individual by individual basis is not sufficient; such consideration ignores the problems created by conflicts of privacy. Most, if not all, of the data with which we are concerned is the joint property of at least two parties -- the person who originated the information, and the person whom the data concerns. In many cases, the privacy rights of these two parties conflict. Consider the case of medical

records. Included in these records are many impressions that the doctor might note to aid himself in his future work with the patient. For example, it might be very important to record that a patient showed indications of schizophrenia. The physician would not want the patient to be aware that this opinion was recorded in the medical record. Thus, to release the medical record for examination by the patient would conflict with the physician's right to professional privacy.

2.4 The Legal Viewpoint

The formulation of a legal definition of privacy, either by statute or precedent, is as difficult a problem as the development of a semantic definition. Within the context of our democratic institutions, certain rights are specifically guarenteed by the Constitution. However, privacy was not explicitly mentioned in that document because it was less a problem then than it is now. Although a number of Constitutional bases for the right to privacy exist in the First, Fourth, Fifth, and Fourteenth Amendments, the interpretation by the courts has varied from case to case. However, guidelines have been developed by the courts along which the legal implications of privacy issues can be evaluated.(14) One of the most important and far-reaching of these is the concept of the chilling effect that invasions of privacy tend to impose upon the exercise of civil liberties.

The chilling effect, as defined by the courts, is

the tendency of individuals to view invasions of privacy, especially surveillance activities, as a threat to their exercise of free speech or other activities explicitly protected by the Constitution. Such invasions of privacy may assume many forms. It is the indirect effects of these invasions that the courts have viewed as unconstitutional.

The courts have developed three primary guidlines by which a given chilling effect may be ruled unconstitutional (3). These guidelines are:

A. The severity and scope of the alleged chilling effect on the exercise of First Amendment freedoms.

The difficulty of proving the chilling effect under this guidline is indicated by the case of the United Public Workers vs. Mitchell:

> "...the general threat of possible interference with those appellants' rights by the Civil Service commission under its...rules does not make a justiciable case or controversy. A hypothetical threat is not enough."(3)

Logically, of course, the chilling effect is not dependent upon actual infringement of civil liberties. If an individual perceives a threat of infringement, his activities are chilled whether or not such a threat actually exists.

B. The liklihood of opportunities to vindicate, with reasonable promptness, such First Amendment rights as may be infringed upon. The courts seek only those cases which involve reasonable elapsed times since the violation of rights occurred, and seem to imply that they

want to establish a statute of limitations for such violations.

C. The nature of the issues, which a full adjudication of the merits must resolve, and the need for factual referents in order to properly define and narrow the issues. There must exist a clear factual relationship between the alleged violation of privacy and the corresponding First Amendment right.

It should be clear from this brief discussion that these guidelines place stringent constraints on an individual's ability to legally prove invasion of privacy. In paragraphs below, we will show that advancing technology is severly compounding these difficulties.

2.5 The Society's Viewpoint

Dr. Westin's definition emphasizes the fact that society desires to enforce its norms upon individual members. Such enforcement is, of course, inherent in the definition of "society"; very few people would question the necessity of such enforcement to the existence of civilization.

In order to enforce norms, society establishes a variety of institutions which watch over individuals and monitor their behavior. Thus cumulative social pressure places constraints on each citizen's privacy decision. We cannot choose, for example, to drive cars at excessive speeds, or to burn down our neighbor's house.

In the absense of explicit legal and semantic

definitions of privacy, however, the institutions for norm enforcement are not themselves sufficiently constrained in their actions. Institutions may therefore exceed the bounds of reason quite by accident in their zeal to carry out their assigned tasks. Numerous examples of such excess may be found in the press.

The seriousness of these excesses is compounded by the public's lack of sophistication in making the privacy decision: many people are completely unaware of the implications for information dissemination that their actions have. Obtaining a credit card, for example, represents consent to release quite a considerable amount of personal information to a system whose control of access is relatively poor. Such information as salary, bank balances, and marital status become available for distribution.

3. INFORMATION COLLECTION: THE REASONS

All of this is not to say, of course, that society has no right to collect information about its members. Civilization could not exist without such collection. What has been lacking is a framework within which to discuss why data is collected.

There are three main forces which drive men to collect, analyse, and disseminate information. These are: 1) to facilitate the management function of society; 2) to help resolve conflicts of individual's rights; and 3) to disseminate information for its own sake. Most invasions of privacy can be traced to the fact that a particular system

is collecting data for more than one of these reasons, or is collecting data relevant to one reason and distributing it for another.

3.1 The Management Function of Society

Perhaps the most suceptible to abuse is the collection of data to facilitate the management function of society. In order to maintain a complex civilization, a tremendous coordinating effort must be undertaken on a continuing basis. For example, in order to distribute paychecks to employees considerable information, including his earning rate, his hours of work, his social security number, his home address, and the number of his deductions must be known. It is difficult to quarrel with the necessity for keeping this information.

The most common abuse is over-extension. The collection of information has a very powerful driving force inherent within itself -- the third force for collection. Data collection systems, if left alone, will often collect data far beyond their true needs and collection will become a goal in itself rather than a means to a specific end. Questions such as "Taking things all together, would you say you are very happy, pretty happy, or not too happy these days?", when asked of senior citizens by the Census Bureau (6), are clear examples of over-extension.

3.2 Conflicts of Individual Rights

The second driving force for data collection is to set up systems for resolving conflicts in the rights of

individual members of the society. For example, it is clear that driver's licenses are necessary in order to prevent dangerous, incompetent, and reckless persons from abusing other people's rights to use our roads with some measure of safety. Another good example is the FBI fingerprint file, which is tremendously helpful in preventing the destruction of life and property by criminal elements.

Perhaps the most common abuse of such systems is dependence on the relative political power of the groups whose rights are in conflict. Such systems must be constructed carefully to avoid the possibility of might being right. To construct such a system clearly requires that the agent making the final judgement not be subject to political pressure.

3.3 Dissemination for Information's Value

The last major reason for the collection of information is the inherent value of information in its own right. The common expression "knowledge is power" retains its validity in the fast paced and highly politicized climate of our society. Perhaps the best example of such a system is education.

In systems which are built for the purpose of dissemination, care must be taken that information is not inappropriately disseminated. For example, the library should not open its files of user's borrowing records to examination by the general public.

It is especially important that systems which

logically exist for one of the first two purposes not be allowed to disseminate information for its own value. Such dissemination is almost always inappropriate. For example, probation records are maintained in order to resolve the conflict between an individual's right to be given a lighter sentence and society's right to be protected from dangerous criminals. To release such records to prospective employers (for either money or political favors) is an illegitimate invasion of privacy.

We are now in a position to delineate the most important aspects of the privacy decision (see Figure 1). On the one hand, there are society's needs for information, and on the other, there are the individual's needs for privacy. The data collection decision must be a tradeoff between these sets of needs.

The Privacy / Data-Collection Decision: Social Benefits vs Social Costs

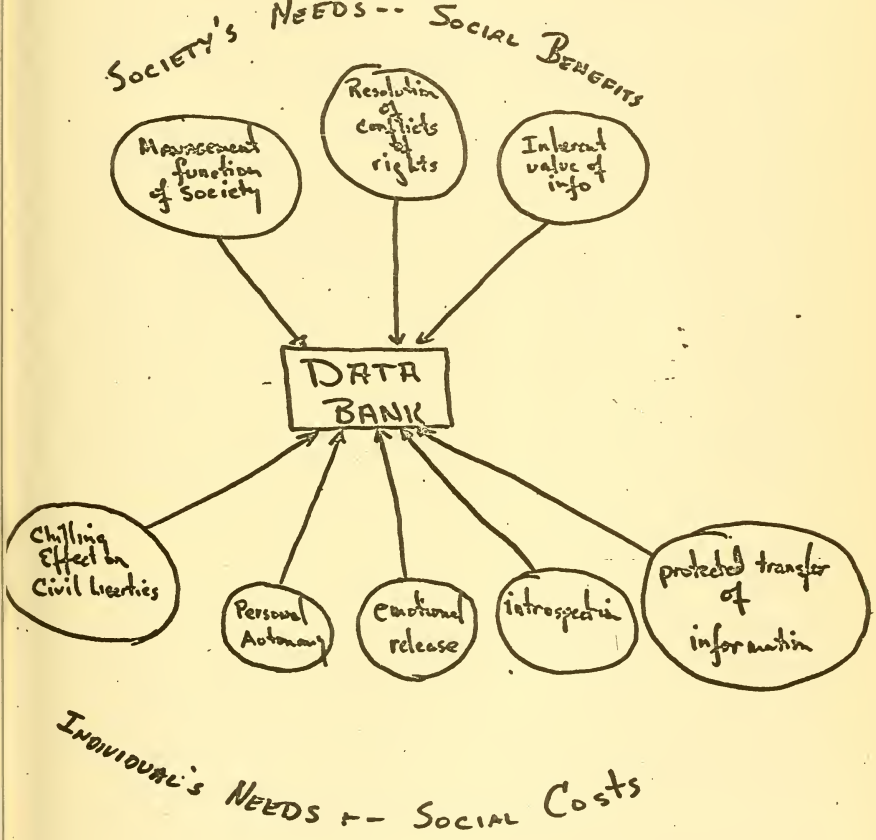

Figure 1.

4 METHODS OF DATA COLLECTION

The means by which information on individuals is collected are numerous and varied; they range from very unsophisticated to highly technical methods.

The most obvious means to obtain information from people is simply to ask them questions. Surprisingly, very few people refuse to answer questions on such topics as income, sexual behavior, political and religious beliefs, and educational background, if only the questions appear in some "legitimate" form (i.e. questionnaires, voter opinion surveys, and the like). People are equally willing to divulge information about the drinking habits and marital behavior of their neighbors. It is clear that too few people question the validity or necessity of requests for information. Simple questioning without coersion or pretext is the major means by which invasion of privacy occurs.

A second, and less direct, technique for obtaining information is to search readily available public sources, such as town records and published information including books, newspapers, and unofficial reports of various organizations. Sometimes this information must be purchased; the Internal Revenue Service, for example, has had a policy of selling to anyone lists of all persons in the U.S. who own registered firearms.

The third method of information collection is physical and psychological surveillance. This involves the use of manpower and, at times, electronic equipment to

monitor a person's activities.

Of course, the flow of information may go considerably beyond the person to whom it is first released. When existing and future databanks become interconnected, one of the most important sources of information will be other databanks.

5 PRIVACY AND TECHNOLOGY

Technological development has increasingly important ramifications for privacy; the rapid advance of science and technology carries with it a hornet's nest of problems. Perhaps two developments have most strikingly demonstrated the conflict between privacy and technology in the United States -- sophisticated electronic communications equipment and the high-speed digital computer.

5.1 Communications Equipment

Electronic communications equipment presents a challenge brimming with implications for privacy. The capability for electronic bugging and surveillance on a massive scale has been developed. Moreover, industrial espionage in the U.S. is at least as big a business as government domestic intelligence operations. For example, a 1967 study performed by the Saber Corporation, which specializes in anti-bugging devices, conservatively concludes that industrial espionage accounts for annual losses of more than three billion dollars. (1)

At least as important as the proliferation of surveillance devices is the proliferation of

telecommunications equiment. Our ability to re-distribute data around the country at high speed enables us to propagate violations of privacy far and wide long before anyone becomes aware of the problem. Current plans for nationwide integration of some telecommunications networks present tremendous privacy problems which no one has yet addressed.

5.2 The Computer and Privacy

But bugging devices only facilitate the collection of raw data. The most powerful device yet developed for the accumulation and processing of that data is the computer. However, the computer itself is not an invader of privacy; it is only an amplifying device for man's ability to process data. It becomes a major factor in the problem by virtue of the magnitude of that amplification.

Consider, for example, the IBM System 360/195. It is capable of performing on the order of twenty-five million calculations per second. In terms of storage capacity, the mass storage unit marketed by Precision Instrument Company of Palo Alto (an argon-laser device) stores 645,000,000 bits per inch. Thus one 4800 foot reel of computer tape could contain about twenty double-spaced typewritten pages on every person in the United States. File retrieval time for such a system would be less than four minutes.

The greatest progress in computerized privacy protection has come about rather indirectly through the advent of multiple-access time sharing systems. The

development effort for these systems requires protection of one user's information from accidental or purposeful access by other users. Considerable effort on access control systems which permit controlled sharing of resources in the multiple-access environment has been undertaken by a variety of research projects such as M.I.T.'s Project MAC. (4),(7),(8)

Partial protection is provided in many time sharing systems by the requirement that the user identify himself at the terminal. Schemes ranging from simple passwords to signature recognition have been proposed or implemented. These static schemes suffer from the fact that any identification must be converted to a bit pattern for transmission over data lines to the computer; thus the user's I.D. may be had simply by tapping his phone line and recording the transmission. A more effective scheme, in which the user's password is the answer to a computation performed on a string of random digits supplied by the computer, is now in use at Project MAC. Since the user's password is different at every session, it is safe from tapping.

However, tapping of data lines will still enable the theft of transmissions of data. A number of effective schemes for encoding and decoding transmissions have been developed, but none are in widespread use.

Within the computer's storage system, the problem is one of permitting controlled sharing of programs and

information. Access control schemes vary widely in their sophisticaiton; the only systems which offer even reasonable protection are implemented in academic computer facilities. Perhaps the most successful scheme to date is that employed by Multics at Project MAC, in which protection is attained through control of access paths to information coupled with a ring structure which offers the ability to specify the level of privilege of any program with respect to others in the system. Even this structure, however, does not solve all access problems.

Another consideration is the fact that the same centralization of information and computing power that makes time-sharing systems cost-effective may very well make concentrated efforts to break the access control system cost-effective. Centralization may therefore be expected to cause an increase in the number and persistence of attacks on the access control system; its integrity becomes a very important issue.

5.3 Technology and the Courts

This advancing technology is rapidly destroying whatever competence the courts have had in dealing with privacy issues.

The main problem is the speed with which information can be dispersed. The irreversible damage done by illegitimate dissemination of adverse information, coupled with the courts' inherent delays, means that preventive measures cannot be taken, and that corrective

measures would come too late.

Moreover, any penalties which might be promulgated would require considerable technical knowledge to enforce. Given the present technical sophistication of the judicial branch, the job of executing the sentence would necessarily fall to the same programmers who implemented the system in the first place. Such dependence upon the good will of the guilty clearly is no solution to the problem. For example, the contents of a data bank which has been ordered destroyed might well be stored on microfilm before the order is carried out.

Presently the world of the courts and the world of data processing have very little in common. No satisfactory laws exist for the protection of privacy from advancing technology. Even if such laws are passed, a stupendous effort will be required to bring the rest of the legal system into the computer age.

6 A FRAMEWORK FOR ANALYSIS OF SPECIFIC DATA BANKS

Having examined the nature of the problem of privacy, it behooves us to develop a clear analytical framework for viewing individual databanks. The objective of such an analysis is to develop criteria for the design of specific databanks. The analysis assumes, of course, that careful consideration has previously been given to the question of whether a databank is needed at all; a data bank which does not serve one (and only one) of the three reasons for collecting information should not exist.

The concepts discussed in the following paragraphs and the relationship among them are illustrated in Figure 2.

FLOW of INFORMATION : PRIVACY ISSUES

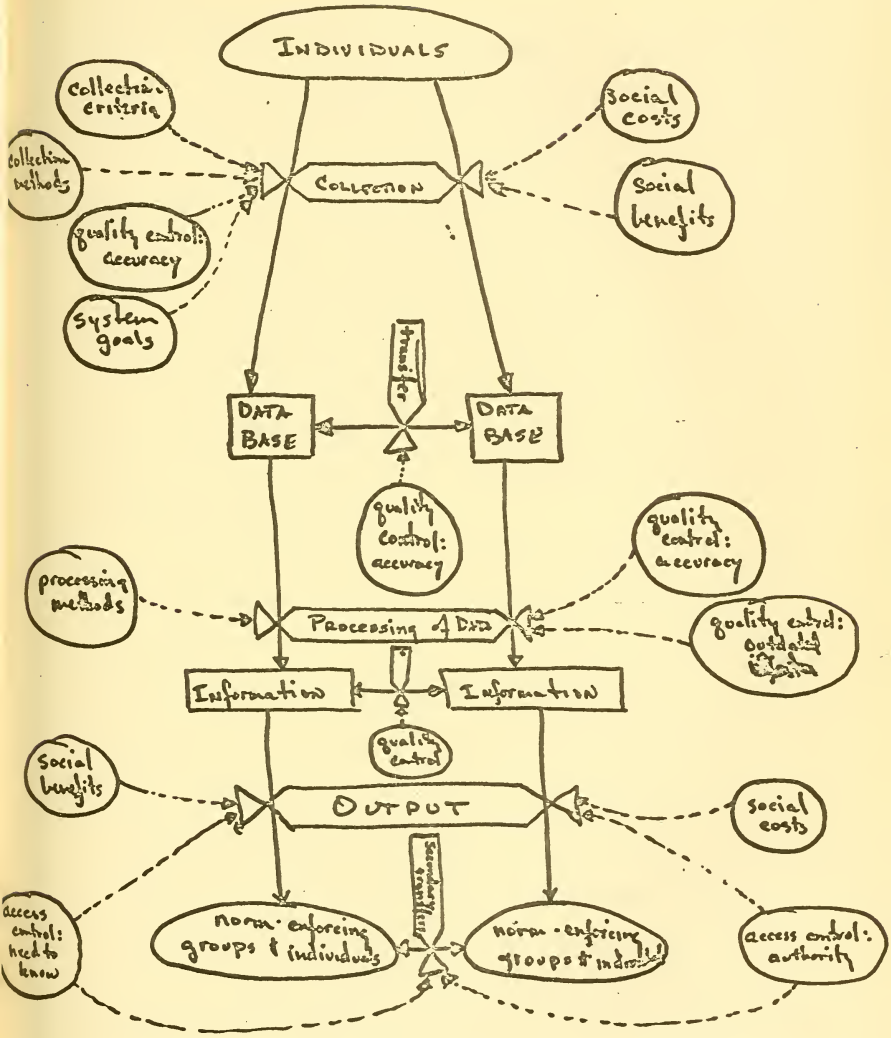

FIGURE 2.

6.1 Collection Criteria

Unless there exists the possibility of a chilling effect on civil liberties, the collection of data is not of itself an invasion of privacy. The majority of information is collected through acceptable channels and for justifiable purposes. Among the most commonly developed databanks are company personnel records, national census data, and industry statistical information. Only when information is collected through inappropriate channels, is disseminated to unauthorized persons or organizations, or is utilized for an inappropriate purpose has privacy been violated. Once the decision to establish a data bank has been made, the control of the collection and distribution of information becomes the central issue.

Of primary importance is the criteria by which data concerning an individual or a group becomes a candidate for entry into the databank. In order to establish a comprehensive and logical set of criteria, prior thought must be given to the specific goals of the system. If the desired output can be stated precisely (and justified on the basis of the rights of individuals and groups to control their own privacy), then input criteria can be defined and bounded in a fashion that not only eliminates the gathering of useless data and promotes efficient system design, but also prevents unwanted side effects.

Failure to clearly define the objectives of the databank is a contributory factor in improper collection.

When a failure to specify objectives occurs, any information which might be of remote relevance at some time in the future is collected. This usually results in the collection of considerable unnecessary information and in a potential threat of invasion of privacy.

6.2 The Quality of Information

Once reasonable standards have been established for determining what data is to be sought as input to the system, it is necessary to set up procedures for controlling the quality of that information.

Quality control has two aspects. First, the accuracy of input data must be controlled as it is entered. In a computerized system, this might involve checking punch cards for keypunching errors.

The second aspect of quality control concerns the removal of information from the file when it becomes outdated. Perhaps information related to individuals (and corporations) should be classified like radioactive metals -- by "half lives", with different lengths of retention time depending on the nature of the information.

6.3 Data Analysis

The next important consideration is the methodology used for aggregating raw data into a usable product. The collection of data by itself produces very little in the way of useful managerial information. Data must be analysed and manipulated into a usable format; data are the building blocks of information. The methods used in

this analysis determine precisely the content of the output information. Improper methods may result in biased, misleading, or false information being transmitted by the system. Such information may well constitute an invasion of privacy.

6.4 Access Control

Given a system which is able to provide useful information, it is necessary to carefully control access to that information. Virtually every piece of information is sensitive to some degree and requires protection against unauthorized usage. Specific rules for the dissemination of information which consider both the authority and need to know of any potential user must be established. But the promulgation of these rules must be accompanied by procedures for enforcement.

6.5 Inter-databank Transfers

A further problem that must be considered is the exchange of data between databanks. First, care must be taken to insure the propriety of such exchanges. Moreover, interchange demands verification of the accuracy of any transmitted information so that errors will not be propagated.

6.6 Social Effects

Finally, the social effects of any proposed information system must be considered. Each function that the system is to perform must be weighed in terms of its social benefits and social costs. The benefits may be

delineated in terms of the driving force behind the system's establishment--will the system in fact assist in the management function of the society; will it help resolve conflicts of individual rights; or will it cause progress through the distribution of knowledge.

These benefits must be balanced against the social costs of the system, which may be measured in terms of the individual's loss of privacy, the resulting degradation of freedom and the possible chilling effect on the exercise of civil liberties.

7 AN INITIAL SOLUTION AND ITS SHORTCOMINGS

Today the most commonly proposed solution to the problem of privacy is simply to allow individuals access to their own files in order that they might correct any inaccurate information. This proposal is over-simplistic for several reasons.

First, the idea assumes that the individual is the only entity which might be harmed by an invasion of privacy. This is, of course, not the case. There are many groups who have been harmed by the illegitimate release of information -- large corporations, draft-resistance groups, political groups, and the Government itself. Although it is true that consideration of individual rights must take precedent over consideration of organizational rights, these groups presumably have some right to privacy. However, Constitutional guarantees are even less well defined for organizations than for individuals.

Second, individual access assumes that the individual is necessarily the person most qualified to correct his own record, and that he will be interested in having his file current and accurate. Again, this is a false assumption in many instances. It is ridiculous to think, for example, that a person should be able to change his medical record at will. Moreover, in the case of information which in some way is unfavorable, it will never be in the individual's interest to have correct information in his file. If we do not trust a small group of people to accurately report sensitive information, then we surely cannot trust everyone, en masse, to perform this function.

The most important shortcoming of this solution is that it does not recognize the problem of conflicts of privacy. To show the patient his medical record would compromise the doctor's privacy; to show the student his letters of recommendation would compromise the authors' rights to privacy. Clearly giving the individual access to his own files is an inadequate solution to the problem.

8. OTHER SOLUTIONS

8.1 Separation of Fact from Opinion

The first attempt at a solution to the problem of conflicts of privacy might be to draw a very clear distinction between information which is to be considered fact, and that which is to be considered opinion. In the medical example, it would be possible to separate the objectively provable facts from the physician's opinions,

giving patients access to the former, but not to the latter, record. Unfortunately, this distinction between verified factual information and interpreted or heresay information is not drawn in many databanks. Moreover, even if it were, there would still remain conflicts of privacy.

8.2 Other Alternative Solutions

Careful consideration should be given to Senator Sam J. Ervin's proposal to:

> "create a Federal agency with powers to register all data bank operations, military and civilian, to demand justification for the records kept and to enforce a citizen's right to examine and to challenge data which could hurt his reputation, even his ability to earn a livelihood, for the rest of his days."(15)
> (See also (5))

The investigative powers of such an agency, however, would be such that the operations of that agency would, in itself, be an invasion of individual and organizational privacy. As a result, such an agency would require explicit guidelines directing the agencies and databanks for which, and by whom, an investigation would be performed. Specific criteria for the evaluation of databanks would be needed to enable investigators to conform to the intentions of the regulatory agency. An additional problem unique to this proposal is the determination, for the regulatory agency, of what data files that agency itself would keep in its investigative files. The entire problem of regulation by a Federal agency is complicated even further by the necessity for both a legislative definition

of privacy and a national consensus as to the extent of each citizens' rights. This quite possibly is a question that only the Supreme Court and the Congress could answer.

An alternate, though related, solution is to establish private companies specializing in the review and analysis of databanks. These companies would perform in a manner similar to Certified Public Accountant firms. In reviewing a databank the firm would need to determine: A) the needs of managerial functions in the organization; B) the legal basis for individual privacy; C) the tradeoffs desired between privacy and society; and D) technological factors.

To perform objectively, these firms would have to be free from political and non-professional pressure, and from involvement in the special interests of the firm whose databank is under investigation. The necessity for uniformity and control of the subjective determinations that would be required if such firms were organized implies legislation either at the national or state level.

The complexity of the problem precludes any quick and simple solution. Other alternatives, beyond those discussed here, need to be developed and studied from an operational and feasibility viewpoint.

9. SUGGESTIONS

Every individual must consider the central questions of privacy which determine his interaction with society. But managers have an even more complex problem in

weighing the advantages and disadvantages of decisions to collect information. The complexity of the problem is highlighted by the decision to utilize advanced technology and the numerous trade-offs involved in such a decision.

Some general guidelines may be provided, however. They are valuable both to the manager faced with an information-privacy conflict, and to the individual citizen considering the central questions of privacy in a technologically advanced society. These guidelines can be summarized as follows:

A. A comprehensive national policy is needed. This policy should only approve of a databank if it serves a legitimate need of the organization. Moreover, this policy must weigh the social benefits against the social costs. There are three identifiable catagories of social costs: 1) direct costs in resources to the organization; 2) cost due to the chilling effect; and 3) cost due to the danger of misuse. Six issues must be evaluated in weighing these costs: 1) the criteria for inclusion of data in the file; 2)control of the quality of the information; 3) control of the nature of data processing and selection of the data to be processed; 4) control of access to the files and technological questions of program access; 5) the degree of centralization in the files; and 6) the degree to which the information system is interfaced with other systems. In terms of benefits, it should be noted that it is important not to hinder an organization in the fulfillment

of its legitimate functions. For example, the Internal Revenue Service should not be prohibited from the collection of tax-related financial information on individuals and organizations.

B. A means for enforcement, carried to the lowest levels of affected organizations, is required as an integral component of any solution to the problems of privacy. Moreover, legislation is required to establish grounds for legally demonstrating invasion of privacy. This legislation should be designed as a deterrent to the illegitimate accumulation of information.

C. A review of existing databanks and information systems should be undertaken by all organizations maintaining such files or systems.

However, legislative and judicial action at all levels is not enough; individual citizens must be made cognizant of the issues and solutions that this paper raises for consideration. True, system builders must be educated in the variety of technical considerations for protection of privacy and given incentives to use them. Incentives for further research should also be provided. But the job of protecting our privacy lies not only with the systems programmer and with the computer manufacturer; it lies with us. Only by increasing the sophistication of each citizen in matters regarding his relationship to the society in which he lives can we prevent "freedom" from becoming an empty word in America.

* The authors wish to gratefully acknowledge the assistance of Dr. Richard S. Morse and Dr. Robert M. Fano, both of M.I.T., who provided invaluable assistance in the research which forms the basis for this paper.

REFERENCES

(1) Brown, Robert M., The Electronic Invasion. John F. Rider Publisher, Inc., New York, 1967.

(3) Columbia Law Review, "Chilling Effect in Constitutional Law". Volume 69/5, May, 1969.

(4) David, E. E. and Fano, R. M., "Some Thoughts About The Social Implications of Accessible Computing". Proceedings of the Fall Joint Computer Conference, 1965.

(5) Ervin Jr., Sam J., "The Computer and Individual Privacy". Congressional Record, Volume 113, Number 37, March 8, 1967. Washington.

(6) _____"Computers and Individual Privacy". Congressional Record, Volume 115, Number 184, November 10, 1969. Washington.

(7) Fano, Robert M.,Implications of Computers to Society". Paper presented at the Kiewit Computation Center Dedication and Conference, Dartmouth College, Hanover. New Hampshire, December 2-3, 1966.

(8) _____"Computers in Human Society-For Good or Ill?". Technology Review, Volume 72, Number 5, March 1970, Massachusetts Institute of Technology, Cambridge, Massachusetts.

(9) Gallagher, Cornelius E., "Technology and Society: A Conflict of Interest?", Congressional Record, Volume 115, Number 55, April 1, 1969. Washington.

(10) _____"Personal Privacy, Data Security, and a Free America". Congressional Record, September 23, 1970. Washington.

(11) _____"Science, Privacy, and Law-The Need for a Balance". Congressional Record, August 18, 1966. Washington.

(12) _____Speech before the American Management Association, March 8, 1968, New York.

(13) _____Speech before the Ninth Practicum on Practical Politics, May 7, 1968, Jersey City State College, New Jersey.

(14) Miller, Arthur R., "Personal Privacy in the Computer Age". Michigan Law Review, Volume 67/6, April, 1969.

(15) New York Times, December 27, 1970.

(16) Playboy, Interview with Arthur J. Goldberg.

(18) Sprague, Richard E., "The Invasion of Privacy and a National Information Utility for Individuals". Computers and Automation, January, 1970.

(19) Westin, Alan F., Privacy and Freedom. Atheneum, New York, 1967.

(20) _____"Life, Liberty and the Pursuit of Privacy". Think, Volume 35, Number 3, May-June 1969, Armonk, New York.

(21) _____"Computers and the Protection of Privacy". Technology Review, Volume 71, Number 6, April 1969.