1968

Computers, Data Banks, and Individual Privacy

Richard Ruggles

John de J. Pemberton Jr.

Arthur R. Miller

Symposium: Computers, Data Banks, and Individual Privacy†

The following symposium transcript is intended to explore the possibility of National Data Banks and the various problems and dangers of such systems. The participants discuss the need for improving the accessibility of data and the countervailing personal privacy considerations.

I. *ON THE NEEDS AND VALUES OF DATA BANKS*†

*Richard Ruggles**

A. The Nature of Privacy

The privacy of the individual has been profoundly affected by the structural changes which have been taking place in American society during the last 50 years. Increasing urbanization and mobility have significantly altered the relation of individuals to each other. Proverbially, anything that happened to anyone in a small town immediately became public knowledge. The movement of the population to large urban centers and increased mobility and ease of communication has, oddly enough, increased privacy in certain dimensions. Neighbors in apartment houses often do not know each other, and the automobile and the telephone have made it possible to choose one's friends without regard to proximity.

The change in the family structure has also altered individual relationships. The child is separated from the family at an early age and spends much of his time in school and extracurricular activities with other children. The husband com-

† From the Fourth Cohen Ethics Symposium held on May 2, 1968 at the University of Minnesota School of Business Administration and sponsored by the Merrill Cohen Memorial Fund and the Graduate School of Business Administration.

* Professor, Department of Economics, Yale University.

mutes to work and the wife engages in social or economic activities of her own choosing. Grandparents and other relatives generally do not live with the family unit, but instead maintain separate households supported by social security, pensions, and other assets saved up over their lifetimes. In fact, one of the most frequent complaints of grandparents is that they never hear from their children or know what is going on. Once the children go off to college or to work, they withdraw from the family unit and begin to develop their own groups of friends and associates.

Personal privacy in these terms has been substantially increased, mainly because fewer people are interested in knowing about an individual's private life. This unconcern, of course, has its disadvantages as well as its advantages, and does not necessarily reflect an improvement.

On the other hand, at the same time that the depersonalization of society has tended toward increasing privacy, there has been a substantial increase in recorded information about the individual. This recording starts at birth and continues until death. There are many types of public records, and many of them are open to anyone who wishes to consult them. If one buys real estate, it must be registered. City directories list the names of individuals and businesses. Phone books provide people's names, addresses, and phone numbers. The individual wishing to obtain a driver's license must provide identification information, sometimes even fingerprints and photographs. If he receives income, he must make out an income tax return. His employers must report information about him to social security. More recently, medicare has added to the records to be filed.

In addition, various government organizations keep their own records. The police maintain files on individuals with whom they come in contact. The FBI may investigate any individual for security clearances or suspected criminal activities. The army maintains records on all individuals who pass through it. Schools keep records on all students. Employers maintain files on employees, and credit agencies build up credit information on individuals and businesses.

The existence of all these records has produced a feeling of insecurity which is easily understandable. The individual is afraid that information, or what is perhaps even more serious, misinformation, may be used against him without his knowledge. The present concern with the right to privacy has two quite different aspects. On the one hand, the increasing concern over

civil rights has made it glaringly evident that in the past the normal process of operation of the society has violated the privacy of many individuals. In many instances police practice in investigating crime or handling minor civil disturbances was not overly concerned with the protection of individual privacy. Recently, greater care has been taken to protect the individual's rights in such situations, despite charges that such action is tying the hands of law enforcement officers. There is little doubt that this concern is a reflection of increased awareness that less privileged groups have a right to be treated in the same way as the more privileged groups.

On the other hand, the privileged groups are seeing their privacy eroded by the increasing information requirements of a growing bureaucracy. Wealthy individuals may resent having to report all of their financial dealings to the government, and pure food laws, safety standards, fair employment practices, etc., are taken by many to be an invasion of privacy. There is a feeling that an individual should be free to run his own affairs as he sees fit without the interference of the government.

B. The Use and Misuse of Information

It is quite obvious that the operation of our modern society does require a vast amount of information. The questions which must be answered about this information relate not only to whether specific information should exist, but also to how it is used—or misused. Some information or misinformation may be useless or even harmful, and some information which is essential and useful is subject to misuse. It is in these contexts that it is proper to talk about the invasion of the privacy of the individual.

In certain areas we frankly recognize that information is in the public domain. Thus, when an individual provides a biographical sketch for *Who's Who*, he is releasing this information to the public. Similarly, if he publishes articles or books, his name will be associated with this material in the future. Bibliographies are part of the information in the public domain. Even listing one's phone number in the telephone book provides a public record open to all. Unfortunately even such public recording of information does permit misuse, as when advertising concerns build address lists from public sources for mass mailings or telephone solicitation. Recently, court cases have indicated that for certain classes of mail—*e.g.*, obscene matter—a person can have his name removed from such private

lists. Many people would gladly remove their names from all junk mail and telephone solicitation lists if it were possible to do so. But few are willing to go to the length of asking for an unlisted phone.

In other areas individuals give up privacy quite willingly because they are assured that those to whom they give information are working on their behalf. Thus an individual will reveal to his doctor or lawyer information which he considers to be of a highly confidential nature. Our legal system recognizes that such information is privileged and need not be divulged under any circumstances.

In still other areas the individual provides information because he recognizes that it is a necessary part of the system. Few would argue that motor vehicle license information is undesirable. Social security information is necessary for the social security system to operate. Even income taxes are a necessary part of modern life, but release of income tax information for any other public or private use may well constitute a serious invasion of privacy.

Besides government records, schools and employers maintain records on those associated with them. Again, these are recognized as necessary, despite the fact that such records may have an important role in determining the individual's future. In some of the larger companies, unions have recognized the importance of records on employees, and much of the grievance machinery relates directly to what is permitted to be put in the record of an individual. In the case of school records, their use, for instance, for determining draft status has been hotly contested as an invasion of privacy.

There are other areas of information about which individuals are considerably more suspicious, and where the invasion of privacy is much greater. We are assured that for purposes of national security certain government agencies must have the power to interview individuals about other individuals, and collect information in considerable detail from any source possible. The question of the use of eavesdropping, wiretapping, etc., to obtain this information has been raised, but the content of the information itself has not been seriously challenged.

Similarly, credit agencies compile information on millions of individuals and furnish such information to any private group desiring to know about the credit-worthiness of an individual, without any control over the sources, methods or quality of the

information obtained. Unfortunately, the individual does not have the opportunity to confront or correct the rumors and misinformation filed in his dossiers. There can be no doubt that this situation constitutes a major invasion of individual privacy, and should not be tolerated.

C. The Need for Information About Our Society

The information needs of society are not, however, confined to the day-to-day operating uses where information about particular individuals is used for administrative actions concerning those individuals. To an increasing extent, we need information about the operation of the society itself in order to understand the social and economic problems which exist in our nation, and to devise policies aimed at changing underlying conditions.

In the physical sciences the importance of information has long been understood. Scientific laboratories exist in order to generate data which can promote the further development of scientific knowledge. The vehicles which we launch into space have as one of their primary missions the sending back of vast amounts of information to enlarge our knowledge. The science of oceanography represents a systematic attempt to assemble information about the ecology of this area of our natural environment. In recent years the observations of weather for meteorological purposes have produced a vast flood of data that has greatly increased our ability to predict weather and our knowledge in this area. Much of the acceleration in the pace of technological change is directly attributable to the ability of scientists to gain access to the kind of information required for a better understanding of major scientific questions.

The operation of the social and economic system has generated masses of data concerned with the day-to-day functioning of the system, and some facets of this data have been used to develop economic constructs. Our national accounts use these constructs to tell us about such things as the rate of economic growth, the movement of prices, and the gold drain. In addition, various government agencies publish masses of aggregated statistical data, much of which is difficult to comprehend but which nevertheless does throw partial light on some aspects of some problems.

The social scientist, unlike the physical scientist, has not been oriented to the systematic use of information. Social sci-

ence disciplines are largely based on theoretical structures that are non-operational and rest for the most part on intuitive feeling and casual empiricism. Where empirical research is undertaken, it generally tends to concern itself with observations of global aggregates or with very small samples of data to which the social scientist may have obtained access.

This situation is not of the social scientists' own choosing. The kinds of information required for an understanding of the social system have not been available, and prior to the development of the computer would not have been usable even if they had been available. The net result, however, is that we have been woefully ignorant of the nature and operation of our economic and social system. For example, we do not know very much about the incidence and nature of poverty. Until recently, the image of the poverty group in the public mind was associated with laziness and lack of moral fiber, and poverty was considered by those not directly concerned to be largely of a person's own choosing. The civil and social disorders of the last several years have made clear that these views are not in accord with the facts. It has become evident that the poor come from initially disadvantaged groups, and that special efforts will have to be made to correct the underlying conditions. But we still do not really know who the poor are in terms of their underlying characteristics, and without such knowledge, it is difficult to develop policies which will be successful in eradicating poverty.

Similarly, we do not really understand the process of inflation, despite our attempt to design fiscal and monetary policies to control it. For example, we do not know whether prices rise in response to rising demand or to rising wage costs. Our knowledge of what causes wage increases is similarly obscure. Do wages rise because of a low unemployment rate and labor scarcity or are wage increases determined by a collective bargaining process where increases in the cost of living or high profits are the main considerations?

Our knowledge of structural unemployment is also deficient. To what extent does general prosperity provide employment for the less advantaged groups? To what extent can retraining programs cure structural unemployment, or are regional development programs required to provide employment opportunities? Recently, the minimum wage rate has been raised, and the charge has been made by some that this in itself will cause further unemployment among those who would be worth hiring at the

lower rate but are too costly at the higher rate. Comprehensive basic information is needed before the impact of minimum wage legislation in helping to alleviate poverty can be evaluated. More recently, proposals for a negative income tax have been made, but again it is difficult to see what effect such policies are likely to have without highly detailed information about the precise economic and social conditions of those who would be affected.

Another example is the problem of the aged. It is obvious that the lot of the aged has considerably improved over the last 20 years, but in spite of this many still live in what is essentially poverty. In order to design future legislation, it is important to know whether the increasing levels of income and the spread of private pension and health insurance plans coupled with the present social security system and medicare will in fact substantially reduce the problem of poverty among the aged in the next decade or so.

In giving examples of the types of problems which need investigation so that we can improve the society we live in, I have mentioned only some of the major economic problems. Other social scientists—psychologists, political scientists, and sociologists—could suggest many other problems relating to such things as civil rights, mental health, and crime—all of which may require highly detailed and comprehensive information about our society.

At the present time only fragments of economic and social data exist in any one place, and access to even this information for research purposes is difficult. The individual government agencies are essentially operating organizations concerned with carrying out specific tasks, and are generally unwilling to permit their current operations to be disrupted for research purposes. What is needed is to bring together the data from many different sources so that they can be made readily accessible for research purposes, and so that individual pieces can be fitted together to provide a comprehensive picture of the operation of our society. Accordingly, it has been recommended that a National Data Center be established which would be the repository for the basic data of the different government agencies, making these data available for use in economic and social research.

From the point of view of the government, the establishment of a National Data Center might well reduce the amount of information which would have to be obtained from individuals and businesses. Under the present decentralized system, each

government agency obtains its own information so that individuals and businesses often find themselves providing slightly different versions of essentially the same information time and time again. The establishment of a National Data Center might well reduce the redundancy of the statistical system, and at the same time improve the consistency and coherence of the information, thus providing better information at lower cost to both the individual respondent and the government.

D. The Need to Control the Collection and Use of Information

The threat to individual privacy through the collection and misuse of information exists irrespective of whether information is brought together in one central location. Some of the most flagrant abuses that have occurred in recent periods are due to government agencies demanding what is essentially improper information. In one case school children were given questionnaires asking whether their parents quarreled. Employees of some government agencies were asked detailed questions concerning their political views and their personal affairs.

Unfortunately, at the present time many government bodies conduct their data gathering activities with considerable independence and little supervision. They have considerable freedom in hiring investigators to collect information from other government agencies, private business, and private individuals, and they are free to exchange information with other groups.

It is small wonder, therefore, that a sense of uneasiness about privacy exists. Furthermore, as already indicated, the individual does not have access to information about himself, so that the misinformation produced can never be corrected. One should not be under the illusion that the perpetuation of the existing highly decentralized system without controls provides any protection for the individual. The greatest harm that is done to the individual is in precisely those agencies and private organizations where information collection is unhampered and secretive, and the information is used against the individual in terms of decisions which seriously affect him.

In contrast with this quite unhappy situation, those agencies concerned with the systematic compilation of data operate quite differently. The Census Bureau, for example, has no operating functions and therefore takes no actions of any nature with respect to individuals. All of its records, furthermore, are confidential. No other government agency, congressional committee, or other body has access to the individual records of the

Census Bureau. This confidentiality rule has been upheld by the Supreme Court. Thus, for example, the Internal Revenue Service cannot even get the lists of individuals or businesses covered by the Census, since this might turn up names of individuals who have not filed tax returns. Congressional committees conducting investigations cannot use information provided by the individual or business to the Census Bureau, even if there are copies in the files of the business. Every business and individual, furthermore, knows precisely what information is held by the Census Bureau. Public hearings are held on the questions which are to be asked on Census forms, and there is public debate as to what specific items should be included.

If we are to correct the present abuses which do constitute invasion of individual privacy, the system of decentralized data files should not be allowed to continue. Explicit consideration should be given to precisely what kinds of information different government agencies should be permitted to gather and keep, and steps should be taken to see that the confidentiality of information is protected and its misuse prevented.

The only systematic way to undertake such a reform is to set up an independent non-operating agency specifically concerned with the task of monitoring the information system and preventing its abuse. One of the first requirements would be to exclude from the files of all government agencies improper information which is now entered. Although the complaint would be heard that this would result in the loss of important sensitive material needed for crime detection or security purposes, this same charge has been made in the past with respect to the question of the admissibility of certain types of evidence in the courts. Thus, for example, confessions obtained improperly have been ruled inadmissible. In similar manner, casual rumors obtained by interviews with neighbors might also be considered improper for inclusion in an individual file.

In any event, as has been suggested by both Professor Charles Reich at Yale and Mr. Pemberton, every individual should have a right to see the information contained in files relating to him. The independent non-operating agency should in fact be concerned with enforcing compliance by government bodies with standard codes developed to protect the rights of individual privacy.

At the same time, it would be possible for such an agency to bring together for statistical and research purposes the basic files of the different data-gathering agencies. This does not

mean, of course, that anyone in any agency could push the proverbial button and get any information he wished. The Internal Revenue Service still should not be able to get lists of names of individuals who respond to Census enumerators. Similarly, individual tax return information should not be made available to other government agencies.

For statistical and research purposes, however, it should be possible to tap the basic information of all agencies in order to further our knowledge about the conditions and operation of our society. Thus, for example, although medical records are of the most sensitive nature, studies of cancer in relation to air pollution might well find it useful to process medical and demographic data together in the interests of scientific research.

In conclusion, I would like to reiterate the following major points. First, the existing situation is one in which there has been a substantial encroachment on individual privacy by many public and private organizations. Second, much of the failure of our social and economic institutions to cope with the major problems facing the nation is directly attributable to the inadequacy of the information relating to our society. Third, a continuation of the present highly decentralized information system will not cure present abuses, but will prevent the integration of information required for future social and economic development. Finally, an independent non-operating institution should be developed which is charged with the proper development of economic and social information and with protection of individual privacy through restricting access to information and the elimination of improper information.

If we do create such a National Data Center, which can not only provide the necessary base for research on the central economic and social problems now confronting us but can also provide a safeguard against encroaching bureaucracy, we will be taking a major step forward.

II. ON THE DANGERS, LEGAL ASPECTS AND REMEDIES

*John de J. Pemberton, Jr.***

I want to underscore the significance of what I have heard: the advocacy of the use of modern and efficient means of gathering, storing, and retrieving data, to deal with social problems; and at the same time the advocacy of a new and increasing

** Executive Director, American Civil Liberties Union.

sensitivity to the invasion of rights of individuals occasioned by any system for gathering, storing and retrieving information.

Professor Ruggles is right, the problems are there now. They do not arise out of the introduction of efficient means of dealing with data. In fact, we may, as his National Data Bank proposal suggests, become more systematic in our methodology of protecting the rights of individuals just because we do move from inefficient to more efficient means of dealing with data. But we shall have to be determined to do so, for the hearings conducted in Congress on the Budget Bureau's data bank proposal in 1966 and 1967 have suggested that many proposals in this area have been insensitive to individual rights.

Simply, I think two major rights of an individual are apt to be violated by someone gathering information about him; and it may be particularly dangerous if it is the government that does so. The first is the obvious invasion of his right of privacy. I am *not* speaking about the danger that the information gathered about him may be inaccurate and unfairly prejudicial. I am saying that even accurate information may be unfair or an unwarranted invasion of his privacy, because it is information which he is entitled to keep to himself and those to whom he intentionally discloses it.

Take a young man in the 1950's who, in his student days in the 1930's, had joined an organization, later discovered to be a Communist front, and had been immature in his judgments and about his continued political association with that group. We saw throughout the 1950's the unfairness that could occur to him from the inferences the public drew from what might have been perfectly accurate information as to what he did in the 1930's. Absent systematic methods of surveillance of other people's political activity, as well as storage and effective retrieval of that information, the ordinary course of a healthy democracy has been that people grew up politically without having what they themselves later came to judge as political mistakes live as skeletons in their closets to haunt them indefinitely. At least such mistakes did not haunt them in such irrelevant matters as private employment which was unrelated to their political activity.

The other danger is one related to inaccuracy of information. It is the danger that is represented by the experience many people have with the gathering of credit information: Anyone in the world who is somewhat persistent can find a great deal of credit information about you, except you yourself. If you try to

find a credit report on yourself you may have enormous difficulty. There is the example of the New York legislator who was denied a mortgage loan and persisted in requesting information from the bank to which he applied until he learned that a credit rating bureau in New York reported him to be a bad risk because of a default judgment that had been taken against him. Only perhaps because he was a state legislator could he bring enough pressure to bear to get *accurate* information on what the credit bureau was saying about him. It turned out that another man with a similar name did indeed have a default judgment rendered against him. But unless he knew what was in that file, it was impossible for the error to be corrected. It was impossible for him to do anything to prevent being harmed by inaccurate information which was being circulated about him.

All of these problems are present in existing data collection and dissemination systems. What we fear, perhaps unreasonably, is the efficiency that may be introduced by modern methods of collecting, storing and disseminating the information.

In June, 1967, an enterprising reporter for Newsday magazine decided that he wanted to find out what he could really learn about somebody in one of the communities within the circulation area of his magazine. He picked a name at random from the telephone book, called the man and said, "I'd like to use you as the guinea pig in my experiment," telling him what the experiment would be. "Do you have any objections?" The man said, "Oh no, there is nothing to worry about." He then spent several weeks examining public records concerning this individual with whom he had no prior contact. After gathering the material, the reporter published a profile and biography of this otherwise anonymous individual living in the Newsday circulation area. The man about whom he wrote the biography screamed in pain, "where did you get that kind of information about me?" Every item was in a public record. There were birth records, marriage records, and health records. There were records on his children kept by the educational system. There was recorded financial data regarding his application for mortgages on his car and his home. He was a veteran of World War II and had recorded his discharge papers. And yet this is only part of the story that could have been collected with the kind of central data bank that we are now discussing.

What we seem to have done is rely on inefficiency to protect our privacy—to protect us from these particular dangers—and we suddenly realize that we can no longer do so. I agree with Professor Ruggles, we ought not to have been relying upon it at all. We are susceptible to injury by anyone who wants to work hard enough to do so, and this will continue to be true unless we take steps to discriminate among the *kinds* of information that are gathered and stored.

That much can be done to improve the functioning of many social programs was underscored by a recommendation of the Research Division of United Planning Organization, a private community action agency dealing with social problems and poverty in some areas of Washington, D.C. It was suggested that services important to the action components of the agency could not be performed unless it was permitted to organize a genuine data bank, which ultimately would have to be computerized in order to handle the volume of information to be collected. Something short of a data bank would give the agency the capacity to render some descriptive research services to the board of directors and the action planners of the organization, but would not permit it to evaluate the kind of impact that they were making on the community.

The information sources that would be available to such an agency, in addition to their own inquiries—studies of the communities or neighborhoods that they were operating in—would include police records, records of the educational institutions, welfare agencies and private agencies. Information so collected might answer such questions as: Who are the school dropouts? What is the relationship between dropouts, juvenile arrest and juvenile court records? Yet, it would be easy to create anonymity for such data by collecting all of it without identification, or destroying the identification of individuals after it was collected. However, this is not feasible when the data is to be kept alive to show a moving profile of the neighborhoods and communities that are being serviced by the agency, to show whether new social conditions are changing the problems that the agency is dealing with, or to show whether the actions of the agency itself are having some impact, affirmative or negative, upon the various existing social problems. To keep the information alive and current, it is necessary that new information about the same individuals be introduced into the data. As soon as this occurs, the possibility of destroying private individual identifications is eliminated. New information about

Johnny's relationships with the police cannot be introduced unless it is related to, or put in the same file or pigeon hole with the old information about Johnny. How then, the Research Division asked, are we going to do anything to protect the privacy of individuals? Are we not asking their consent to assemble information that the police may have on them with information that other sources may give us, despite great possibility of injury to them as a result?

After several pages describing how this problem of protection was wrestled with, it was proposed that all information assembled and kept be put on two decks of IBM cards, one deck dealing with identification and another deck dealing with substantive information. The two decks would then be separately put on computer tapes. A committee would control the identification and substantive decks, and the tapes on which they were placed, rather than any one man. Members of the committee would have to act in concert in order to put together the substantive and the identification decks for purposes of adding or abstracting information. This alternative was recommended even though it would cost a fairly small organization an additional $6,000 in capital outlay and an additional $200 a month to operate as compared to a nonprivacy-protecting system of data collection and dissemination.

What I am suggesting is that only as the advocates of modern methods of information storage and retrieval couple their advocacy with concern for the individual's right of privacy, protection against false information, and confrontation of information being stored about him and the opportunity to correct it—rights that can only be protected with additional expense and delay—will we have this kind of protection. I commend Professor Ruggles for being such an advocate.

III. ON PROPOSALS AND REQUIREMENTS FOR SOLUTIONS

*Arthur R. Miller****

When I was invited to participate in this symposium, it was suggested that my remarks occupy the "middle ground" between Professor Ruggles and Mr. Pemberton. Accordingly, in

*** Professor, School of Law, University of Michigan. Professor Miller indicates that many of the ideas in his remarks before the symposium will be set out in elaborated form in a forthcoming article in the Michigan Law Review.

thinking about today's session my plan had been to listen to my symposium colleagues, synthesize the remarks of the preceding speakers and then go on to formulate this so-called "middle ground." Now that I have heard Professor Ruggles and Mr. Pemberton, I find the "middle ground" fully occupied and feel myself technologically unemployed. I thus would like to spend my allotted time extemporizing to reinforce some of the points previously made and perhaps indicate my own philosophical bias in this debate.

The title of the symposium has the word "computer" in it, and I think it would be well for all of us to leave the hall later this afternoon with some concept of what it is that this computer is capable of doing to us in the area of individual privacy—in particular, what is so unique about the computer that distinguishes it from the traditional manila folder?

The computer is a many-splendored animal. It is myopic to think of it as little more than a high speed calculator with a gland condition. It's much more than that. Modern information transfer technology in time will prove to be the heart of a new communications network, a communications network that differs from many of the communication networks that we are familiar with, such as telephones, telegraph, radio, television and newspapers, only in technological and media terms. Accordingly, the computer must be dealt with as a communications network.

Just as we decided over 30 years ago that we couldn't tolerate airplanes flying randomly over the United States and that we couldn't permit radio stations to broadcast indiscriminately and without regard to the question of allocating the radio spectrum, so it is that we will shortly find, indeed I believe that the FCC has already found, that we can't permit unregulated computer transmissions, especially if computers are used to transmit sensitive information over long distances to other computers or data centers. This is not a fanciful concern. In this day of Early Bird and Telstar satellites, we are capable of moving information from the great libraries and museums of Europe to the United States on a computerized basis in a very short period of time if we choose to do it. The future of global information interchange is almost limitless.

But to focus more closely on the subject of today's symposium, in what ways might this new technology with its many wondrous uses pose a threat to individual privacy? Perhaps a few examples of computer applications will present the computer-privacy dilemma in a more graphic fashion. In a medical center

in the South, doctors are implanting heart patients with sensors that permit the patients' bodily functions to be monitored by computer. The object, of course, is to develop some type of an "early warning" system for the prediction of heart attacks. The theory of the experiment is to try to ascertain what chemical or biological changes take place inside the human body immediately before the onset of the attack so that the patient can be treated before he is rendered moribund by the attack itself.

Elsewhere, there are plans being formulated to provide everyone with an identification number at birth. As a practical matter, most of us already have identification numbers that serve a variety of purposes. Our social security number currently is used to identify us for tax purposes, by the military, and in many institutions of learning, including my own, it also serves as a student identification number. The obviously desirable goal of all this is to develop a system of record keeping and information reporting that avoids much of the existing duplication that Professor Ruggles alluded to, and to provide a central locale at which all information can be accumulated about every individual, whether it pertains to social security, taxation, military, immigration and naturalization, or medical condition. Thus, the day may come when an American falling ill while away from home will contact a local doctor in France or Japan who will pick up his telephone, dial the patient's identification number, and immediately be given his medical history so that the doctor can be aided in diagnosing the problem and avoiding drug reactions.

Wonderful! There is no doubt that these applications of computer technology are socially desirable. But the same sensors that can be implanted into the human body to develop a medical early warning system can also be used in order to track people, to monitor their movements, their activities, and in the fullness of time, if we believe some of the modern theories about thought and intelligence, to compute and determine what they are thinking about, what their aggression level is, and what their criminal potential might be at any particular moment in time. It already has been suggested that we take advantage of the fact that we keep convicted criminals incarcerated for long periods of time by analyzing their body chemistry and behavior patterns. The object would be to permit the implantation of sensors into these people upon their release from prison in order to keep track of them as they move in society. Thus, when com-

puter monitoring shows that they are undergoing a deviation from their normal body chemistry or behavior pattern which might signify an increase in their aggression potential, the police could be dispatched to prevent the subject from indulging in any antisocial activity. Similarly, the identification number, which can achieve so much in the way of record keeping efficiency, also can act as the key to an individualized, computer-based dossier that can constitute an informational leash around our necks along the lines suggested earlier by Mr. Pemberton.

In short, I am suggesting that we are dealing with a problem of immense importance this afternoon. The basic thesis I would like to leave with you is simply that given the large stakes, we should not think simply in terms of the ethical or moral implications of a National Data Center, or any other type of a data center. We must recognize that we are dealing with a new technology, whose applications are just beginning to be perceived and whose capacity to deprive us of our privacy simply cannot be measured in terms of existing systems or assumptions about the immutability of the technology.

I should make one thing clear at this point. I do not oppose data centers. I am overwhelmed by their capabilities; I am concerned about their proliferation; but I think it is absolutely ludicrous and unrealistic to advocate the elimination of a modern technology that can carry out important governmental and nongovernmental operations simply because that technology might be abused. Given the complexity of modern society, given the society's commitment in terms of billions of dollars and billions of man hours in the fields of education, urban renewal, social welfare, and natural resource development and allocation, we simply have to face the fact that in order to effectuate many of our programs we must have and be able to process amounts of information that far exceed anything we have ever contemplated dealing with before.

To draw a rough analogy, we are all cognizant of the destructive capability of the automobile. We know it can kill and maim people. Nonetheless, no one seriously advocates the banning of automobiles from the highway. Rather, the quest is to develop a rational pattern of regulation of vehicles and operators to ensure that we derive maximum social utility from the automobile at a minimum of social cost in terms of injury to persons and property. I suggest that this should be the goal of those who interest themselves in the question of computers, computer technology, and the right of individual privacy—ra-

tional regulation of computers and computer applications in those contexts in which individual privacy might be affected.

Professor Ruggles made a very, very cogent point which was seconded by Mr. Pemberton, and is worth repeating. The problem of privacy and information gathering has always been with us; indeed it is a natural and inevitable by-product of a literate society. The problem simply has not been focused upon before because of our preoccupation with physical surveillance—the snooper, the guy who rummages through your house or office at night, the fellow who trails you on the street, the user of the parabolic microphone, the dispenser of the olive in your five o'clock martini that is really a transmitter.

Moreover, in the past informational privacy has not been a major concern because it has been protected by a number of factors unrelated to technology. Large quantities of information about individuals simply have not been available, and the data that has been available has been difficult to procure without the type of investigation into an individual's career that Mr. Pemberton described earlier. Typically, information has been decentralized; it has been highly superficial in character; and access to it has been difficult to procure. In addition, we live in a mobile society in which people are very difficult to keep track of, and recorded information often is difficult to locate. Finally, by-and-large, most people are unable to interpret and infer revealing information from the data they can get.

Now, I think this is the point at which I depart somewhat from Professor Ruggles' analysis. As he points out, there is little doubt that we have a highly imperfect system today in terms of our files and confidentiality. Neither the federal government nor the states has done an effective job of protecting us against the intruders in our society. A reading of the hearings held by Senator Long's Subcommittee on Administrative Practice and Procedure and Congressman Gallagher's Special Subcommittee on Privacy reveals that snoopers have used a variety of electronic gadgets and more traditional methods to turn our society into a transparent world. Nonetheless, I don't think that the current unsatisfactory situation regarding privacy invasions by traditional means should obscure the fact that the computer adds an entirely new dimension to the privacy problem, and I'd like to spend a few minutes describing some of the peculiar privacy concerns raised by the computer.

Ever since the federal government entered into the taxation and social welfare spheres in the 1920's and 1930's, greater quan-

tities of information have been sought from citizens and corporations. Moreover, in addition to the normal governmental processes of gathering information, in recent years access to government employment and other forms of governmental largess increasingly has depended upon a willingness to divulge private information. In other words, we are being compelled to give the government and other data collecting agencies information that traditionally we were not obliged to reveal. Furthermore, as recording processes have become cheaper and more efficient, the tendency toward information gathering has intensified and has been accompanied by a tendency toward centralization and collation. I think we are witnessing something akin to a Parkinson's law, which can be stated as follows: As capacity for information handling increases, there is a tendency to engage in more extensive manipulation and analysis of reported data, which in turn motivates the collection of data pertaining to a larger number of variables.

I think that at this point in time the computer is the keystone to the continued application of this form of Parkinson's law. Perhaps the best example of this trend and the relevance of the computer is provided by the census proposed for 1970. The 1970 census asks numerous questions, some of which contain one or more subquestions and many of which are highly personal in nature. For example: How many showers have you in your home? How many beds do you have in your house? Is your home subject to a mortgage? How do you heat your home? How many children have you had, including stillborn (this is asked of females)? What were you doing in April, 1960? The 1970 census represents a continuation of the trend toward longer and more complex questionnaires. It seems to me obvious that the availability of high speed, relatively inexpensive machine processing acts as an incentive to this continued proliferation of the census.

Yet the Constitution, which authorizes the census, doesn't say anything about gathering information concerning showers, beds, personal finances, modes of transportation, and many of the other subjects covered by the proposed questions. I am not suggesting that the government does not have a legitimate need for this information, because the case can be documented for the utility for most of the sought-after information. The further and more significant question, however, at least in my mind, is what price are we willing to pay in terms of citizen privacy to allow the government to get some of this information?

If we assume an increasing level of information gathering and processing on the part of the government and the more extensive use of computers and machine handling of data, I think we can posit that the following risks, which exist under current information handling techniques, will be increased: errors in reporting, recording, and indexing data; abuse of information by persons working with the data; misuse by people who are at a distance from the data, but who can gain access to it through remote terminals and modern communication techniques; and finally what may be the most disturbing risk of all, the violation of an individual's understanding that the information he discloses to a particular governmental agency for a particular purpose will be used only by that agency and only for that purpose. The Census Bureau does a marvelous job but it simply does not have control over the individual census taker who goes door to door and acquiesces when one interviewee asks, "say, how did my neighbor Mrs. Jones answer that question about the size of her mortgage?" Unfortunately, in many instances there tends to be a free-wheeling communal discussion of the responses to the questionnaires.

There are additional risks to widespread use of data centers. As information accumulates, the contents of a dossier appears more impressive and there tends to be an increased reliance on information in a dossier despite what may be the basic softness of some of its contents. Our success or failure in life ultimately may turn on what other people put into our computer file, and on an unknown programmer's ability, or perhaps his inability, to evaluate, process, and interrelate information. The electronic record of our endeavors may become a hearsay narrative prepared by a "computernik" much the way our knowledge of the Trojan War and the travails of Ulysses has depended in the main on Homer's filtration of earlier chronicles.

The centralization of information from widely divergent sectors of the government or private industry or academe—the last by the way having an extensive amount of financial, medical, and personal information about students and faculty—also creates problems of information accuracy. At this juncture I am not talking of the literal accuracy of the data; I am talking about contextual accuracy. Information can be entirely accurate and sufficient in one context, and very misleading or incomplete in another context. For example, consider a bare statement of marital status—married, divorced, separated, or single. Consider the significance and different connotations of each of

these words when examined from the perspective of selective service, a credit bureau, internal revenue, immigration and naturalization, social security, or an insurance company.

The problem of context may be graphically presented by looking at one of the most dangerous records being maintained in our society—the unexplained and incomplete arrest record. Consider the citizen whose computerized central file, accessible to law enforcement agencies throughout the land, contains the entry, "arrested June 1, 1942, convicted felony January 1, 1943, sentenced 2½ years Leavenworth." Is it likely that this man is going to get federal employment, or be accorded the same benefits and courtesies that many of us receive from the federal government? Yet I have just read to you a shortened form of the arrest record of a man convicted of being a conscientious objector during World War II. I would hate to see that type of an entry dredged up from the past and put in a centralized file with no concern for who may have access to that file, for its accuracy, or for many other problems and complications.

I would like to present one last, well, second-from-the-last potential "horrible" from the computerized future. As I said at the outset, a computer is not simply a machine in a fixed position in a building. It can be that, but it often will be much more. It can also be the heart of a surveillance system. Thumbing through the reports issued by Senator Long's Subcommittee, one finds marvelous testimony concerning activities in the United States Post Office. Not only do they get the mail to you but on occasion it is given very special handling in the process.

The special treatment is known as the "mail-cover operation." It is a technique for watching suspected Communists, tax delinquents, "undesirables," and, well, we don't know who else. How does it work? A Federal Investigator from the FBI, Treasury Department, or perhaps Narcotics Bureau, is stationed at the Post Office that processes your mail. He just watches the mail addressed to you and the mail being sent by you. He lists the people you write to, and lists the people who write to you. They want to see who you bank with, what stock brokerage house you have, who your friends are, and anything else that might turn up. Actually it's a terribly costly surveillance process.

Well, some day in the near future we will have fully operational optical scanners, which are electronic devices that can recognize and transmit images or information about characters on a page much the way camera lenses or eyes can. When this day arrives, we can replace our human agent at the Post Office

with an optical scanner that gazes down at your mail as it is processed and immediately records the information that is on the envelope—the names and addresses of sender and recipient—transmits the data through the telephone system or microwave relay into the central data bank where it is translated into machine readable information and automatically enters it into the files of the people corresponding with the suspect. All this is entirely feasible once we get a fully operational optical scanner. The Post Office Department in Detroit currently is experimenting with such a device. The official word is that it is just for reading zip codes, but obviously the potential for snooping is enormous.

Finally, I think we have to recognize the fact that a certain element in our population, I won't even begin to guess what percentage, views the development of computer technology, the spawning of data banks, and the use of identification numbers as firm evidence of the increasing de-humanization of man and the increasing de-humanization of American society. These people are becoming active in an attempt to retard this trend. Rebellions against the use of telephone area codes have occurred, zip code numbers are ignored, and I wish I had a dollar for every computer punch card that has been intentionally folded, spindled, or mutilated contrary to its express directions. I leave to the psychologists and the sociologists the task of evaluating how serious a problem this really is. To date very little has been done in the way of research on the subject of the interaction among privacy, the computer, and social environment.

As a footnote to this point let me add that we also should be aware of the fact that increased government surveillance, and I'm using surveillance in the broadest sense and to cover all aspects of the increased pressure to extract information from the citizenry and the taking away of an individual's right to control information about himself, all are bound to have repercussions in terms of our individual conception of what our government is all about. Here again, don't misread me. I'm not predicting *1984*, although others see it as a real possibility. I call your attention to a recent editorial in the *Saturday Review* that carried the headline, "1984, Minus 16 and Counting." I do suggest, however, that we must take account of the pressures on privacy caused by information gathering and data banks and if we are serious about our government being a form of benevolent, outer-directed, social control, I think we have a lot of fences to mend in this regard.

I have spent a great deal of time simply describing some of the risks of data centers; Mr. Ruggles has previously suggested some of the pathways for protection. At this time, I would like to second these suggestions because I am not, as I said at the outset, arguing against data centers; I am arguing against the irrational, unstructured growth of data centers and pleading for a maximum intellectual input into the question of the impact these data centers may have on our traditional notions of privacy. And that, of course, is what I think this symposium is all about. How can we guarantee individual privacy and at the same time not deprive ourselves of the wonders of this new technology: Hopefully, we can spend some of the panel time developing this subject further. As for now, I think I shall halt this stream of consciousness.

IV. GENERAL COMMENTS

The following comments were made by the participants at the conclusion of their initial remarks.

(Professor Ruggles) I would like to comment on the use of the social security number. The assignment of a number to an individual, I suspect, is going to go out of existence pretty much. For example, in the Econometric Society we started out computerizing our records by account numbers, but it was so hard for the girls to learn these or look them up, that we finally decided we might use names. This turned out quite well, since the computer can recognize a name as well as a number. Now it is true that you sometimes have duplicate names. What do you do about this? Well, you identify them by where they live, their location and so on. If you have people with the same name living in the same location, you can add little descriptors like their age. It is far simpler to use names than numbers and we may find that the computer instead of mechanizing us further is going to adapt to us. I agree, however, that when records are kept by name and the computer has access to them the privacy problem is much more serious.

Now as to the question of whether the computer has expanded our information, in 1940 I purchased from the Census what I thought to be a duplicate set of punch cards of the 1940 census with all the questions asked. There were some 40 items. (Actually, the number of demographic items collected on a 100 per cent basis in our census is not a 100, it's six. All of the rest are on a sample basis. It is just too expensive to collect

all this data on everybody. We also do a 25 per cent sample on housing and other things which give us a wider base of information.) I thought I was purchasing a duplicate deck. They were very cagey; they sold me the originals. And for many years I kept these up at Yale in 96 cartons. There were over a million cards, and just this last week the Cowles Foundation said they needed more room and asked me to please get them out. Now they are being put on tape, but this just shows how the data does hang on—even pre-computer. As for the scanning of the Post Office, I agree that this is of the same nature as wire-tapping, and if we outlaw wire-tapping, we should probably outlaw this practice too. But I do not feel this has anything to do with the problem of centralizing information. This is just a practice which new technology makes possible on a partial basis, namely in the Post Office Department, and information so acquired can feed into a decentralized FBI file as well as a centralized one. The fold-bend-mutilate sort of thing is, of course, done on a non-technological basis by students who write exams for me. Every now and then the writing becomes so illegible that I can't possibly make out what the student is saying. Naturally, he hopes I will give him the benefit of the doubt and not mark him down. If I did he would come back and say, "See this is exactly what I said." So trying to 'mess up the system' works at all levels.

One final word. Originally I opposed the term "data bank" because it was so much like a data morgue. But the more I think of it, the more I think that this is an appropriate term, for this reason. With an account in a bank, you can put money in and you can draw money out, other people can put money in and draw it out, the bank is pretty careful that you do not draw somebody else's money out. Similarly, there has to be some sort of regulation as to how things go in to the account, what is acceptable, what your credit rating is and so on and so forth. It does seem to me that if we adopted the policy of not allowing any of the major agencies to keep their own records, but rather required them to deposit their information into a central file and then to draw it out according to their need, this might be a better process.

The New York State Identification and Intelligence system does, in fact, operate on this principle. Prior to the establishment of this system there were seventy million files in the New York State System. Some 3,700 agencies kept individual files, and employed some 66,000 individuals. Eight million

searches of these files were made each year for some three million violations. So it was a large business. When they had the Appalachia Raid and tried to get information on one individual, they found that in the neighboring communities within 100 miles there were over 200 separate files on him. What do these files contain? Well, they are kept by Police Departments and so on, and mainly contain newspaper clippings, partial arrest records, interviews, rumors, and little slips of paper. Much of this information would not be sufficiently respectable to put in a system.

The New York Identification and Intelligence System represented a new non-operating agency that took information as it was generated by the various groups and retrieved it for agencies when the request was proper. Eventually it will cover not only police files but those of the courts, etc.

Not all information is proper to give out for various purposes. However, from the point of view of civil rights the New York System is a tremendous advance, because it means accurate, up to date information can be provided for the use that is required. This has meant, I believe, that many people are released on recognizance because an examination shows that they have no prior record. Therefore, you do not have to put them in jail while you investigate to see whether you can let them out on bail. So, in fact, there has been a great deal of improvement, and I believe the number of people released without being jailed has gone up considerably since the system has been adopted.

(Mr. Pemberton) It occurs to me to add, first, that I think that it was appropriate for Professor Miller to inject new problems with respect to surveillance into this discussion of the problems of keeping and disseminating information. I would like to use an example other than the Post Office scanner to make the point. Currently the United States Senate is debating what started out to be the Administration's Safe Streets and Crime Bill. The Administration, far from advocating new authority for law enforcement agencies to wire-tap and to engage in electronic bugging surveillance, advocated new regulations to control wire-tapping and electronic bugging. The Senate Judiciary Committee rewrote the Administration's bill to put in what they claimed would be a controlled wire-tap section, an authorization to law enforcement agencies (federal by virtue of the federal act, state by virtue of permission granted in the proposed federal act to state legislatures) to authorize control of wire-tapping. Far

from being actually controlled it would be an "open sesame" to all kinds of presently unauthorized means of electronic surveillance of individuals by law enforcement agencies. Far from complying with the Administration's request that new techniques for electronic surveillance be met with new laws to protect privacy against these new techniques, the Senate Judiciary Committee has recommended to the Senate that entirely new authority be granted in derogation of the very simple prohibition against wire-tapping in the Communications Act of 1934, and further that broad new authority be granted for *official* wire-tapping.

I'm suggesting that to the extent concerns for privacy, arising out of the existence of new techniques for invading privacy, do not prevail in the current legislative debate, we may be legitimately alarmed about insensitivity to these very human values when it comes to the regulation of collection and dissemination of data and data banks. I would like to suggest also, without impinging on Professor Miller's promise of recommendations, also that the presence of new techniques in data gathering and dissemination warrants regulation of private and government data gathering and dissemination as well as government data banks.

Let me suggest that credit data gathering and reporting goes relatively unregulated in our society today, but it is not a centralized business. If one credit agency makes a disastrous mistake about me, I might possibly be able to get credit from another source that is dealing with a credit agency that doesn't have that derogatory information. If this is centralized, with all of the information about me in one computer in New York, and every credit extending agency can obtain information about me, the danger of damage, irrevocable damage, is considerably greater. It seems to me it is totally warranted, particularly where interstate commerce in credit information dissemination is involved, for new regulations to require that such private endeavors have procedures to insure fairness.

(Professor Miller) I'm afraid I have some bad news for you. The Credit Bureau of America and IBM are developing a computer-based national credit rating system while we sit here and talk. The retail Credit Bureau of Greater New York has records on eight million people in the greater New York area—credit records. They're not computerized as yet, but they will be in the near future—all information agencies are going to be computerized. Each year this credit bureau enters into its file 750,000 derogatory items about one or more of the eight million strap-hangers in New York. Now, you might not be impressed

with this statistic. After all, New York is a large and supposedly evil place. Maybe there are 750,000 bad items about its citizenry. But then you start looking at a breakdown of these items to find out what they are. You discover that the largest single component is an item of about 250,000 entries noting the initiation of law suits against one or more of the eight million people upon whom files are maintained. We all know that a lawsuit, such as a divorce action, or a landlord-tenant squabble, or an automobile accident case, can adversely affect an individual's credit rating or chances of employment, but does this organization check the denouement of each of the lawsuits to protect those individuals who successfully defend against them? No, sir. Only the entries dealing with the commencement of the lawsuits are recorded. The fact that the vast majority of these actions are never prosecuted or result in a vindication of the defendant is unreported.

This illustrates the type of sloppy procedure and lack of sensitivity that we have to be aware of and guard against; and I guess I'm afraid that the New York State Identification and Intelligence System referred to earlier by Professor Ruggles has not overwhelmed me with its sensitivity. One of the first public pronouncements made by its management, indeed a public pronouncement that was repeated before Senator Long's Subcommittee, was the boast that it was going to interconnect and exchange information with other criminal law enforcement offices in the United States. This worries me because I don't trust the quality of a substantial portion of the information gathering in most police bureaus. Indeed, I don't even trust the information gatherers in my own law school, because they make mistakes and often are callous or indifferent to the rights of individuals and ignorant of the ways in which information can injure people.

Let me just add one further dimension to this problem since a question has been raised regarding what originally was called the Right of Privacy Act of 1967, which I fear ultimately will prove to be a tragic piece of reactionary legislation. The computer-privacy issue and the National Data Center should not be viewed in isolation but rather in terms of the overall development in our society of the concept of privacy. By the way, I think the heated debate over whether to establish a National Data Center is a red herring. As a practical matter some system is bound to be developed, although I think enough people have expressed concern so that when it is created there is going to be a reasonable degree of attention to protecting privacy. Actually, a

form of National Data Center has already been established. All you have to do is look at the report recently put out by Senator Long's Committee on the dossiers currently maintained by federal agencies, and you realize that the government has a vast amount of information on each of us that is available throughout the government and to others. Inevitably, each information gathering agency will put its data in a form that is compatible with the form used by other agencies, and information interchange will be accomplished through dial access telephones. This, in effect, will create a National Data Center.

In considering the fate of informational privacy in this country, we must take account of trends other than the National Data Center. A good example of what we must be concerned with is the proliferation of non-federal data systems, such as those being developed in the insurance and credit fields. Information gatherers in these industries investigate a number of private matters that are deemed relevant to mortality risks and credit worthiness, such as extra-marital relations, homosexuality, and outdoor sporting activities. Increasingly, this data is finding its way into computers and more and more these computers are being tied together in networks, which facilitates maximum dissemination of the collected data. In the academic community, each year bigger and better files are developed on students. In every quadrant of industry, tremendous quantities of personal information are being preserved. These data centers will present the really significant problems of computer-based information and privacy in the future. My concern about these centers is intensified because of two recent developments in the law of privacy.

One is the Freedom of Information Act of 1966. That title is a beautiful euphemism. The Freedom of Information Act means that a great number of people have freedom of access to information about you. It's a legislative statement that an extensive amount of the material in governmental files is now available for public view. Now there was a very, very solid justification for enacting this statute. In the past many regulatory agencies have been very secretive about what is in their files and what the rules of the game were—they have exhibited what may be termed sort of bureaucratic anal retentiveness. The Freedom of Information Act is designed to let the public in to see what these agencies are doing. Among other things, however, it provides that people can examine your files in a number of federal agencies as long as access is not covered by specific confiden-

tiality statutes or unless entry to your file would constitute a clearly unwarranted invasion of privacy, and that's approximately the statutory language.

In other words, the statute represents a complete reversal of the traditional presumption in favor of individual privacy. The individual whose dossier has been opened is obliged to prove that entry into his file would be a clearly unwarranted invasion of his privacy. The difficulty is that when somebody delves into another person's records, the latter rarely is told of that fact. So that even when an individual could establish his right to privacy, he may never get the opportunity to do so because he will not know it has been invaded. That is item one.

Item two is a decision by the Supreme Court in 1967 in a case entitled *Time, Incorporated v. Hill.* It involved a play called "The Desperate Hours," which dealt with the travails of a family held captive by three escaped convicts. After the play opened on Broadway, LIFE magazine wrote an article about it stating that it was a re-creation of the story of Jessie Hill who had undergone a similar, but not identical, experience some years earlier. Hill sued, arguing that LIFE had invaded his privacy; that the experience had been a terrible one and that he had moved from Pennsylvania to Connecticut to forget about it; and that the LIFE magazine article had dredged it out of obscurity and made him look ridiculous in the eyes of his community.

Hill won in the trial court and was awarded damages. However, the Supreme Court of the United States, on appeal, held that because the first amendment needs "breathing space," the law cannot recognize a right of privacy in the context of speech by communications media, even when the disseminator erroneously reports the story, unless the erroneous report is issued willfully. Although I have been very simplistic and sketchy in my description of the case, I think it is fair to say that the net effect of the decision is to impair the vitality of the right of privacy in this country.

Another item worth mentioning is the trend I mentioned in my earlier statement—the increase in recent years in information gathering, which will be accelerated by computer-based interconnected networks. If you tie the fact that more information is being gathered by the government with the enactment of the Freedom of Information Act, which permits more people to gain access to it, and add *Time, Incorporated v. Hill,* which held that you may be negligent when you use it, you get some sense of the dimensions of the threat to privacy in this country. All of

these trends must be looked at as a unit because their confluence represents a terrifying specter.

I am beginning to have serious doubts as to the ability of the right of individual privacy to survive in our society unless we start taking stock of the threat and start doing things along the lines suggested in the original Right of Privacy Act. Unfortunately, that proposal, which was designed to cut down wire-tapping, has been transformed into an act that is going to authorize increased wire-tapping. The sad thing about the Right of Privacy Act is not only the fact that its original purpose has been subverted, but also that it never really came to grips with the problems of information privacy.

(Mr. Pemberton) I agree with Professor Miller and genuinely fear that the massive assault on privacy that the confluence of several trends seems to be bringing about at the moment will have to be dealt with by legislation, and not merely by piecemeal accretion of law through individual cases.

(Professor Miller) I think it's very clear that if we sit back and await a case-by-case shifting in the law of privacy, and the adjustment between the right of privacy and the first amendment, we may come to grief before change takes place. In light of the movements in the technology, this process is just too slow. What we need at this point is a total and complete legislative revamping of all phases of the regulations regarding governmental and nongovernmental information gathering, processing, manipulating, and storing. At present we have a crazy quilt of legislative regulation with too many pieces dealing with small aspects of the information gathering process and without any rational overall program. Many of the statutes are inconsistent; they don't cover all the cases and problems that may arise; and they don't take into account the massive shifts in information technology and the new threats they pose.

We need a total and complete revamping of our legislative approach to informational privacy, including the regulation of computer transmissions and the movement of information in interstate commerce. We have to think about encoding and scrambling computerized data; transmission line priorities; and make sure that there isn't wire-tapping of computer lines, which is just as feasible as wire-tapping of telephone lines. Beyond this we simply must regulate the character of information that private agencies can collect. It is necessary to make sure that credit agencies and insurance companies achieve a minimal level of ethical activity in the gathering of information.

The entire spectrum of computer hardware and software manufacturing someday will have to come under regulation, especially since so many systems operate today on a time share basis. These systems present a high risk of monitor intrusion and file stealing because frequently 20 or more different sources input and output data to and from the same computer. Ultimately it may be necessary for the federal government to establish minimal levels of privacy controls in the manufacturing of computers. This is a massive problem that presently is being pecked at by a lot of different people, but I really think that the time has come for some foundation or the American Law Institute to step in and do a complete study.

(Question): *The panel seems to have been unanimous in accepting the notion that data banks are desirable, and I'd like to brave the question as to whether they really are. I want to preface this by saying that if you want to get information about households or individuals say in Minneapolis, it has to be complete if it is to be useful. I submit that it has to fit the specific purpose. It should be accurate and it should cover all periods of time. So I raise the question of whether, even given the capacity of modern computers, it is feasible to create a data bank that will fit these characteristics you've concepted. And then secondly, whether it is as efficient as the present data collection from statistical investigation, where you tailor the investigation to specific purposes.*

(Professor Ruggles) Analysis of information is a complex sort of thing, but much of our information tells us a great deal. For example, supposing we are studying migration—some of our best records might well be social security records which provide an individual's changes in address. Now if you went out to collect and analyze data on migration all over the United States, the cost of making comprehensive surveys which contain the same information as social security records contain would be horrendous.

A number of "matching" studies have been done by census to provide social and demographic information such as death or juvenile delinquency. In other words, the files are set up in such a way that you very often can add information. Much of the information that you say might be collected separately, such as school records and so on, already exists, and our computer capabilities are such today that being able to relate and match the different kinds of information makes it possible to do studies that we never conceived of before.

Let me just cite one case in point: "establishment" data collected by the Census Bureau. When they started putting this on computer tape it became possible to pick up the same establishment year after year and provide a case history. You could examine, for example, the change in wages in various kinds of establishments, and get some understanding as to how much of the wage change in our economy is due to expansion in the higher wage firms because of greater productivity and the discontinuance of this information can be compared with the wage changes taking place in any single firm. To design this information comprehensively for all industries and all regions of the United States is just beyond our capabilities. We have to use a by-product of the system itself.

(Question): *Does the right of privacy exist at all? . . . as a constitutional right?*

(Mr. Pemberton) Does it exist at all as a constitutional right? I don't think we really know. There is language by Justice Douglas in the *Griswold v. Connecticut* opinion—that is the Connecticut contraception case—which tries to piece some sort of a right to privacy out of certain portions of the Bill of Rights. But there is also language in some of the more recent wiretapping cases that seems to run a little bit against the recognition of the broad-gauged total individual right to privacy. I don't think we really know, at least I certainly am not capable of saying yes or no. I think it is in flux at the moment.

(Professor Miller) Could I supplement that simply by suggesting that I think that a number of separate rights of privacy exist rather than a single comprehensive right of privacy as the question may have suggested. Specific rights to certain kinds of privacy have existed in our legal system for a long time. For instance, the fourth amendment's guarantee against unreasonable searches and seizures is a very explicit guarantee of a kind of a right of privacy and it appears in the Bill of Rights itself.

The old law tended to rely largely on property concepts to protect privacy. This is one reason that Eighteenth Century libertarians tended to respect highly the institution of private property. But some kinds of demographic, economic, and technological changes have made property less relevant in protecting privacy. The capacity to eavesdrop electronically is the most dramatic instance of that. If you cease viewing privacy as a single broad-gauge right similar to free speech you discover that our system has had a high respect for privacy in the past—although not always going under that name—and it is a genuine fear that

we are expressing here today; that our system is abandoning today a great proportion of the congeries of values that we associate under the heading of privacy.

(Question) *We have been using the word "information" quite readily throughout our discussion and I am wondering if the solution is anywhere near the real problem. I have been looking at the crutches that we have been establishing relative to the gathering of information as probably being a bigger problem than the gathering of this information itself. In other words, I am wondering about such things as wire-tapping. I can see a group such as this in 1960 B.C. discussing the same type of problem. We didn't have the computer then. We would be discussing how one person could gather information about another by looking in the window, or by transferring data between two people, and we would be questioning what kinds of data he should pass. For example, a minister or priest would have the right to know that a person was committing adultery or was stealing from his neighbor.*

So way back then we had a problem of information gathering about which I am sure there was a group discussing whether they had the right to invade the individual's private life. We have gone through the ages without a computer, but we have had this information gathering problem and there has always existed the danger of twisted terms and abuses by some people. Now people have dispersed and we have a little more privacy. I was just wondering whether the information gathering problem was the wrong area, and if we should be looking rather at the legality of the erroneous data that is being gathered, and concentrate on the legality of protecting the individuals.

(Professor Miller) This is a statement of another approach to the problem, which when added to or in combination with the first approach makes the scheme more effective.

(Question) *What can be done to protect the individual privacy from a bad credit record or a bad civil service record?*

(Professor Miller) Actually, I haven't addressed myself directly to the techniques of protecting privacy against the computer previously because I thought that it really has been brought out by the three speakers in pieces. If you are looking for Nirvana, forget it! If you are looking for a way to sterilize the human race so they don't do any bad things with computerized information, forget it! It can't be done. There always will be an evil programmer just as there are bad lawyers, bad econo-

mists, and bad businessmen who can negate the most carefully conceived protective system.

We have already had experience with this in the programming business. There is a classic case, perhaps apocryphal, of a programmer for a large retailing concern who was doing the programming for the company's payroll. As she was setting up the program for the computerized production of the checks she added a series of commands that directed the machine to send her a payroll check every 18 minutes. Unfortunately, she fell victim to the "pig at the trough" doctrine. She was apprehended because the postman got very tired, and somewhat suspicious, of the enormous collection of mail, obviously containing checks, and he caused an inquiry to be made by the company.

All we can do is play the probabilities in developing controls. First and foremost we need controls on input, and this is precisely what Professor Ruggles has previously addressed himself to, and Mr. Pemberton has supported him. There is so much information about people that we *could* collect and in time it will be economical to collect it in view of the fact that computer costs are constantly declining. But in the case of certain types of sensitive data, we just shouldn't collect it—period! Moreover, we have to start developing a professional cadre in the programming field. After all, we specially train and we license a variety of professions and trades. We have to do the same with programmers who are going to deal with sensitive or personal information.

Another area of protection is controlling access to the data; in many contexts it is essential to identify and limit those who can get into the data bank. This ultimately will be done by using voice prints or finger prints as access keys or identification procedures. We should have a system for monitoring the files whereby anyone who enters or interrogates the system leaves evidence of that fact. Perhaps the system can be designed to record the information that Sam Slick entered the system at 8:18 on such and such a date, that he used the files for a stated number of minutes, and that he looked at and made entries in the files of Bob Boyscout and Dan Dedicated. These records could be periodically monitored to see if any suspicious pattern of abuse is revealed.

We also should give each individual access to his own file and create some type of an administrative structure to enable him to challenge the accuracy of those files. Admittedly such a system would be costly. The FBI and the CIA will be upset and

moan, "Gee, how are we going to catch Communists, subversives and criminals if we have to reveal all our information?" Somebody else will complain that such a system will result in an endless flow of petty squabbles about the accuracy of the files.

Obviously, some accommodations can be made. Cost can be reduced by sending citizens a print-out of their National Data Center file along with their tax forms. There are a number of other things that can be done to facilitate and keep the cost of preserving privacy down but, unfortunately, things will never be perfect.