

Copy 1

THE COMPUTER AND INVASION OF PRIVACY

66062406

137

HEARINGS
BEFORE A
SUBCOMMITTEE OF THE
COMMITTEE ON
GOVERNMENT OPERATIONS
HOUSE OF REPRESENTATIVES
EIGHTY-NINTH CONGRESS
SECOND SESSION

JULY 26, 27, AND 28, 1966

Printed for the use of the
Committee on Government Operations



985486

67-715

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 1966

COMMITTEE ON GOVERNMENT OPERATIONS

WILLIAM L. DAWSON, Illinois, *Chairman*
FLORENCE P. DWYER, New Jersey
OGDEN R. REID, New York
FRANK HORTON, New York
DONALD RUMSFELD, Illinois
WILLIAM L. DICKINSON, Alabama
JOHN N. ERLBORN, Illinois
HOWARD H. CALLAWAY, Georgia
JOHN W. WYDLER, New York
ROBERT DOLE, Kansas
CLARENCE J. BROWN, Jr., Ohio
JACK EDWARDS, Alabama

CHET HOLIFIELD, California
JACK BROOKS, Texas
L. H. FOUNTAIN, North Carolina
PORTER HARDY, Jr., Virginia
JOHN A. BLATNIK, Minnesota
ROBERT E. JONES, Alabama
EDWARD A. GARMATZ, Maryland
JOHN E. MOSS, California
DANTE B. FASCELL, Florida
HENRY S. REUSS, Wisconsin
JOHN S. MONAGAN, Connecticut
TORBERT H. MACDONALD, Massachusetts
J. EDWARD ROUSH, Indiana
WILLIAM S. MOORHEAD, Pennsylvania
CORNELIUS E. GALLAGHER, New Jersey
WILLIAM J. RANDALL, Missouri
BENJAMIN S. ROSENTHAL, New York
JIM WRIGHT, Texas
FERNAND J. ST GERMAIN, Rhode Island
DAVID S. KING, Utah
JOHN G. DOW, New York
HENRY HELSTOSKI, New Jersey

CHRISTINE RAY DAVIS, *Staff Director*
JAMES A. LANIGAN, *General Counsel*
MILES Q. ROMNEY, *Associate General Counsel*
J. P. CARLSON, *Minority Counsel*
WILLIAM H. COPENHAVER, *Minority Professional Staff*

SPECIAL SUBCOMMITTEE ON INVASION OF PRIVACY

CORNELIUS E. GALLAGHER, New Jersey, *Chairman*
BENJAMIN S. ROSENTHAL, New York
FRANK HORTON, New York
NORMAN G. CORNISH, *Chief of Special Inquiry*
CHARLOTTE C. BICKETT, *Clerk*

CONTENTS

	Page
Hearings held on—	
Tuesday, July 26, 1966.....	1
Wednesday, July 27, 1966.....	49
Thursday, July 28, 1966.....	119
Statement of—	
Baran, Paul, computer expert with the Rand Corp., Santa Monica, Calif.....	119
Bowman, Raymond T., Assistant Director for Statistical Standards, Bureau of the Budget; accompanied by Paul Krueger, Assistant Chief, Office of Statistical Standards, Bureau of the Budget.....	49
Dunn, Edgar S., Jr., research analyst, Resources for the Future, Inc.....	92
Gallati, Robert R. J., director, New York State Identification and Intelligence System; accompanied by Eliot H. Lombard, special assistant counsel for law enforcement to Governor Rockefeller, and Edward DeFranco, executive assistant to the director.....	146
Horton, Hon. Frank, a Representative in Congress from the State of New York.....	5
Packard, Vance, sociologist, author, and lecturer.....	7
Reich, Charles A., professor, Yale Law School.....	22
Rosenthal, Hon. Benjamin S., a Representative in Congress from the State of New York.....	4
Ruggles, Richard, Department of Economics, Yale University.....	89
Squires, Burton E., Jr., visiting assistant professor of computer science, University of Illinois, Urbana, Ill.....	135
Letters, statements, etc., submitted for the record—	
Gallati, Robert R. J., director, New York State Identification and Intelligence System:	
Act to amend the executive law, in relation to the creation of the New York State Identification and Intelligence System in the executive department and prescribing its powers and duties.....	169
Association of the Bar of the City of New York, the.....	181
New York State Identification and Intelligence System.....	159
Report of the Special Committee on Problems of Law Enforcement of the Association of the Bar of the City of New York on proposed legislation to amend the executive law in relation to the creation of the New York State Identification and Intelligence System in the executive department, and prescribing its powers and duties.....	180
Report of the Special Committee on Problems of the Administration of Law Enforcement of the Association of the Bar of the City of New York on the feasibility report and recommendations for a New York State Identification and Intelligence System.....	180
Rundquist, George E., executive director, New York Civil Liberties Union, New York, N.Y., letter to Robert R. J. Gallati, director, Identification and Intelligence Project, dated March 18, 1965.....	158
Sturz, Herbert, the Vera Foundation, Inc., letter to Robert R. J. Gallati, director, Identification and Intelligence Project, dated March 16, 1965.....	159
Supplementary statement.....	179
Horton, Hon. Frank, a Representative in Congress from the State of New York:	
Article from the Saturday Review by John W. Macy, Jr., entitled "Automated Government," dated July 23, 1966.....	35
Excerpt from section 139(b) of title V of the United States Code.....	80

CONTENTS

IV

Letter, statements, etc.—Continued	
Michael, Dr. Donald N., professor of psychology and program director in the Center for Research on the Utilization of Scientific Knowledge, University of Michigan, paper entitled "Speculations on the Relation of the Computer to Individual Freedom and the Right to Privacy"-----	Page 184
Pemberton, John de J., Jr., executive director, American Civil Liberties Union, New York, N.Y., statement-----	182
Remarks of Hon. Cornelius E. Gallagher and Hon. Frank Horton on floor of the House, August 18, 1966, on questions of invasion of privacy relating to the establishment of a National Data Center----	311

APPENDIXES

Appendix 1.—Report of the Committee on the Preservation and Use of Economic Data to the Social Science Research Council, April 1965-----	195
Appendix 2.—Statistical Evaluation Report No. 6—Review of Proposal for a National Data Center-----	254
Appendix 3.—The new computerized age-----	295
Appendix 4.—Speech by Vice Adm. H. G. Rickover, U.S. Navy, entitled "Liberty, Science and Law"-----	304

THE COMPUTER AND INVASION OF PRIVACY

TUESDAY, JULY 26, 1966

HOUSE OF REPRESENTATIVES,
SPECIAL SUBCOMMITTEE ON INVASION OF PRIVACY
OF THE COMMITTEE ON GOVERNMENT OPERATIONS,
Washington, D.C.

The subcommittee met, pursuant to call, at 10:10 a.m., in room 2247, Rayburn Office Building, Hon. Cornelius E. Gallagher (chairman of the subcommittee) presiding.

Present: Representatives Cornelius E. Gallagher, Benjamin S. Rosenthal, and Frank Horton.

Also present: Norman G. Cornish, chief of special inquiry; Miles Q. Romney, associate general counsel, Committee on Government Operations; and John Forsyth, special minority consultant.

Mr. GALLAGHER. The subcommittee will come to order.

The Special Subcommittee on Invasion of Privacy today begins its investigation into proposals to establish a National Data Center or Data Bank. The subcommittee is interested in questions of economy and efficiency as they are related to problems of invasion of privacy. The hearings this week continue the special inquiry initiated last year by the House Committee on Government Operations under the authorization of the committee chairman, Hon. William L. Dawson. With me again are the other two members of the special subcommittee, Hon. Benjamin S. Rosenthal and Hon. Frank Horton, both of New York.

Before proceeding with today's testimony, I believe it would be worthwhile to summarize the recently completed first phase of this inquiry by the subcommittee. The investigation centered on three areas: the use of intrusive personality tests by Federal agencies in connection with public employees and job applicants; Federal financial support of research grants and contracts utilizing similar personality tests and questionnaires with children; and a section of the 1964 farm census which asked detailed questions about the outside income and background of all persons living in each farmhouse.

I am happy to report that all of the Federal departments or agencies whose representatives appeared before the subcommittee either have abandoned the use of personality tests, put them on a voluntary basis, or have greatly modified their use.

In addition, Government contractors are now urged to accept the same prohibition on personality tests that the Civil Service Commission applies to Federal employees; and the Bureau of the Census has adopted new procedures to protect the privacy of farmers, members of their families, hired hands and lodgers, when answering questions about outside income in the farm census.

While we are gratified with the successes in these fields, we also are disturbed by other trends within the Federal Government that constitute possible threats to the privacy of American citizens. One such trend is the increasing demand for a centralized facility, within the structure of the National Government, into which would be poured information collected from various Government agencies and from which computers could draw selected facts. It is our contention that if safeguards are not built into such a facility, it could lead to the creation of what I call "The Computerized Man." "The Computerized Man," as I see him, would be stripped of his individuality and privacy. Through the standardization ushered in by technological advance, his status in society would be measured by the computer, and he would lose his personal identity. His life, his talent and his earning capacity would be reduced to a tape with very few alternatives available.

Technology, through the centuries, has enriched human life, and a Federal data center undoubtedly will add to this enrichment and streamline the operation of the National Government. But just as democratic governments historically have secured the freedom of their citizens partly by controlling the fruits of scientific progress, so too must we now make sure that Government computers do not provide the means by which Federal officials can intrude improperly into our lives.

The subcommittee believes it is important that we consider this question before the establishment of a national data center or bank becomes a fact. What we seek at this point is to create a climate of concern, in the hope that guidelines can be set up which will protect the confidentiality of reports and prevent invasion of individual privacy, while at the same time allowing government to function more efficiently and facilitating the necessary research of scholars in statistical analysis.

The problem is potentially serious; its advance solution urgent. It has been reported that funds have already been designated in the 1967 U.S. budget to start a data bank program.

The age of the computer already is upon us. Within the Federal Government alone, it is a billion-dollar business. The Defense Department is devising a computer capable of making 1 billion computations a second. The Federal Reserve Board is gearing plans to make a sharp reduction in check clearance through the use of computers; this in turn will drastically cut the size of the so-called check clearance float. Today's pushbutton telephone will be tomorrow's direct contact with the bank. State and local records are being hooked up on a national scale. Information retrieval in electronic data systems is virtually becoming instantaneous.

Some 20 Federal departments or agencies currently collect and publish data, including the Internal Revenue Service, the Census Bureau, the Office of Education, the Bureau of Labor Statistics, and the Bureau of Old-Age and Survivors Insurance. Information has been supplied to these agencies by persons with the understanding that it will only be used by the receiving agency, for a specific purpose, and in most cases on a confidential basis.

Now, it is suggested that much of this information be pooled in one central source. Presumably, current disclosure restrictions would be adhered to, but the effectiveness of these laws, in some cases, is

dubious. We have even greater fear that the law in some cases is of small concern to those in law enforcement who become overeager in enforcement of that law as they view it. We do not want to see the intended good use of a data center distorted so that it simply makes confidential information more readily available to more people.

Nor do we wish to see a composite picture of an individual recorded in a single informational warehouse, where the touch of a button would assemble all the governmental information about the person since his birth. Such a hypothetical situation could become very real, because into a data bank could be deposited records covering his birth, schooling, military service, employment history, personality traits, credit status, and practically any other aspect of his life. Although the personal data bank apparently has not been proposed as yet, many people view this proposal as a first step toward its creation. I am sure there will be pressures—both within and outside Government—to create one in the future, all, of course, in the interest of economy and efficiency.

The presence of these records in Government files is frightening enough, but the thought of them neatly bundled together into one compact package is appalling. We cannot be certain that such dossiers would always be used by benevolent people for benevolent purposes.

The possible future storage and regrouping of such personal information also strikes at the core of our Judeo-Christian concept of "forgive and forget," because the computer neither forgives nor forgets. We are told that the computer can be programed to program out derogatory and confidential information; what we fear is the ability to program it in.

We also recognize the obstacles that would be cleared away by a data bank for the researcher, when statistics are instantly available at his asking. But we also recognize the danger implicit in such power which would enable a less scrupulous person—or even a well meaning but overzealous Government official—to delve behind the statistics, to the respondent, and learn the inner secrets of an individual. Shall we create an elite who can narrow and dominate the "corridors of power"? And who shall they be?

We also are aware that vast governmental projects are being undertaken to help develop America, and that the Federal Government seeks new information about social and economic conditions to plan and operate these programs. But such programs should not be at the cost of individual privacy.

What we are looking for is a sense of balance. We do not want to deprive ourselves of the rewards of science; we simply want to make sure that human dignity and civil liberties remain intact. We would like to know just what information would be stored in a national data center; who would have access to it; who would control the computers; and, most importantly, how confidentiality and individual privacy would be protected. Thought should be given to these questions now, before we awaken some morning in the future and find that the dossier bank is an established fact, and that liberty as we knew it vanished overnight.

Perhaps new guidelines and safeguards will have to be established to correspond with the sudden development of the computer. Perhaps a new concept in file accessibility will have to be formulated, under

which a person may have the right to examine his own file, or at least have the right of appeal, so that he can insure the accuracy and completeness of his dossier.

These are some of the questions to which we are seeking answers. We believe that once both sides—the need for technological advance and the right of privacy—have been presented before this subcommittee, their inseparability will become obvious, and a sense of balance hopefully will be achieved.

The issue is not whether a statistical data bank can be established nor whether it would be beneficial. A statistical data bank can be established and great benefits can be derived from it.

However, there appears to be a great imbalance between technology on the one hand, and the law and public interest on the other. The issue is, therefore, can we achieve a balance so as to assure that technological progress will serve man and that man's free will will dominate in the new environment that the computer is rapidly bringing about?

Mr. Rosenthal, you have a statement?

STATEMENT OF HON. BENJAMIN S. ROSENTHAL, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

Mr. ROSENTHAL. Mr. Chairman, at the outset of our second series of hearings, I would like to reaffirm my appreciation of your efforts, and Chairman Dawson's wisdom in establishing this special inquiry. I believe we have already had considerable impact—and creative influence which brings honor to the entire Committee on Government Operations, and the Congress as a whole.

My own personal reaction to the proposal for a National Data Center was, I suppose, similar to that of most citizens—intense apprehension at the prospect of still more invasions of personal privacy. In so many areas technological progress is being secured at the expense of personal liberty. The projected National Data Center seems an almost too fitting symbol for that development. And yet, I admit, there is the continual danger of excessive reaction and inordinate fear. For the problem of balancing the benefits and costs of progress is subtle and requires careful study and prudent judgment.

I approach the issue with initial skepticism. I have yet to be convinced of the necessity for a central bank of highly personal data on all American citizens. I have yet to learn why each agency cannot maintain its own files. And I find it hard to believe that the improved efficiency afforded by the Center would outweigh the clear risks.

Even with the most precise safeguards, we must continue to ask ourselves certain basic questions. Is the increased threat to ask our-erty too great a price to pay for the anticipated efficiency and progress? Are we sacrificing too many aspects of our personal lives for limited objectives? Does the additional knowledge we might gain yield benefits to society greater than the losses to the individual?

I intend to ask these questions of all witnesses before this committee. I will not be satisfied with any witnesses who favor the establishment of a National Data Center and who fail to answer such questions satisfactorily. I propose to inquire if adequate safeguards can be formulated so that we can benefit from the growth of technology in

the area of personnel data control. But their development is an absolute precondition to the establishment of any projects such as that before us today. I think I speak for the chairman and for my colleagues in stating that we will tolerate no unnecessary intrusions into the privacy of American citizens, regardless of their source and nature.

Mr. GALLAGHER. Mr. Horton.

STATEMENT OF HON. FRANK HORTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

Mr. HORTON. Mr. Chairman, the mission of this subcommittee, investigating instances of individual privacy invasion caused by or contributed to as the result of Federal Government action, is important and timely. Clearly, our experiences and endeavors of the past year, have proved this point. And I feel your exposition of the subcommittee's work sets forth with special significance the wisdom of Chairman Dawson in chartering this subcommittee.

Privacy, as a fundamental freedom of the American citizen, is an unquestioned constitutional right. That this subcommittee, through examination and exposure, has curbed a brand of overzealousness on the part of certain Government agencies to overlook this right in personality testing is a notable example of the inherent protections to be found in our Federal system of checks and balances.

As significant as those earlier hearings were, I have become convinced that the magnitude of the problem we now confront is akin to the changes wrought in our national life with the dawning of the nuclear age. Proposals to gather in one central location or in one giant data bank all the information which Federal agencies amass on the citizens of this country are sufficiently filled with possibilities for privacy invasion that I believe it is eminently proper for our subcommittee to conduct this investigation.

These data bank concepts are a product of modern technology. Today the computer is a central figure in our society. The increasing rate at which it will change our lives exceeds the imagination, exceeds even the imagination of the computermen who foster it. Dr. Jerome B. Wiesner, dean of science at MIT and former science adviser to President Kennedy, has said.

The computer, with its promise of a millionfold increase in man's capacity to handle information, will undoubtedly have the most far-reaching social consequences of any contemporary technical development. The potential for good in the computer, and the danger inherent in its misuse, exceed our ability to imagine * * *. We have actually entered a new era of evolutionary history, one in which rapid change is a dominant consequence. Our only hope is to understand the forces at work and to take advantage of the knowledge we find to guide the evolutionary process.

We will be fortunate if we are able to keep these processes "evolutionary" and not "revolutionary."

Assuming the best for a moment, let us regard our computer systems as good and fair and the computermen behind the console as honest and capable. Even in these circumstances, there is danger that computers, because they are machines, will treat us as machines. They can supply the facts and, in effect, direct us from birth to death. They can "pigeonhole" us as their tapes decree, selecting, within a narrow range, the schooling we get, the jobs we work at, the money we can earn and even the girl we marry.

It is not enough to say "It can't happen here"; our grandfathers said that about television.

Now, let us compound the concern. Assuming a computerman who was dishonest, unscrupulous or bent on injury, there would be nothing sacred. We could be destroyed.

Adm. Hyman Rickover has expressed a fundamental concept concerning these problems: he states that we must realize that the power of these computers is technology, and technology must serve man; man must never blindly accept technology, he must take up the challenge and control it. It is a force he has to master and use to his benefit.

The admiral exhorts us to be faithful to individual basic values, to preserve our right of privacy and independence and to bend this fantastic new technology to our principles. It is the function of lawgivers, in Admiral Rickover's view, to set the limits within which computermen can operate. He makes it clear that this is not a limit on science or knowledge but only on our use of knowledge and technology.

The concept of such control is ancient. Fire controlled is our friend; uncontrolled it is devastating. The wheel is man's servant and yet his greatest exterminator. The computer is another two-edged sword. It will take more than the controls of the "horse-and-buggy" days to use computers for our benefit and yet keep them from making shreds of human dignity, privacy, and freedom.

To provide an example, despite the flood of technical language some Government consultants use to camouflage their recommendations, the fact remains that a central data service bank would require:

One, that confidential information now in Government files would be forwarded to a new group and used for other purposes than it was originally given; and

Two, that a new group would have the code and would know the names, addresses and background of the people who submitted the confidential information.

Tying the two together would be an easy matter.

It is held that personal dossiers are not intended, but no thoughtful computerman can deny that they are a logical extension of present plans. I am pleased to say that computermen as a group are deeply concerned with the problem of controlling information storage and retrieval so that no one ever will be able to take away our basic freedoms through these means.

One last point: The argument is made that a central data bank would use only the type of information that now exists and since no new principle is involved, existing types of safeguards will be adequate. This is fallacious. Good computermen know that one of the most practical of our present safeguards of privacy is the fragmented nature of present information. It is scattered in little bits and pieces across the geography and years of our life. Retrieval is impractical and often impossible. A central data bank removes completely this safeguard.

I have every confidence that ways will be found for all of us to benefit from the great advances of the computermen, but those benefits must never be purchased at the price of our freedom to live as individuals with private lives.

Mr. GALLAGHER. Thank you, Mr. Horton.

The subcommittee is very fortunate this morning in having as its first witness in this series of hearings Mr. Vance Packard. Mr. Packard is more responsible than any man in our country for alerting us to the dangers that lurk in the twilight of our sophisticated society and the changes that are coming about and creating perhaps a new environment.

Vance Packard, for the last decade, has served as a public conscience for various actions by this Government and business that infringe on individual rights and individuality, largely through such books as "The Hidden Persuaders," "The Status Seekers," "The Wastemakers" and "The Naked Society."

We are indeed honored and privileged to have you open these hearings this morning, Mr. Packard.

Please proceed.

STATEMENT OF VANCE PACKARD, SOCIOLOGIST, AUTHOR, AND LECTURER

Mr. PACKARD. Mr. Chairman and members of the committee, thank you for inviting me to submit my thoughts on the matter of your current concern, the proposals to establish within the Federal Government national data centers.

The chairman has already identified me. I would only say my particular concern has been the impact on the individual citizen of pressures generated by social and technological change, and that my last book, "The Naked Society," was specifically concerned with the erosion of individual privacy arising from these changes and I have talked and written on the basis of later developments which, as you well know, have frequently involved activities within the Federal Government.

I believe your inquiry is an immensely important one. The implications of permitting the Federal Government to assemble in central data banks, or a center, information provided by or about its individual citizens are far reaching. There is clearly a threat to individual liberty in such a project.

Some time ago Dr. Robert Morison, as scientific director of the Rockefeller Foundation, warned:

We are coming to recognize that organized knowledge puts an immense amount of power in the hands of the people who take the trouble to master it.

Certainly we are seeing and hearing that information is power. If this is so, then all of us should be uneasy about the vast amount of information that the Federal Government is starting to store away on its citizens in dossiers, card files, and electronic memory banks.

In recent years we have seen an enormous growth in techniques for observing, assessing, controlling, keeping track of and exchanging information about people. To mention just a few, we have the hidden tape recorders, the lie detectors, the undercover agents, the personality assessors, and the bureaucratic investigators. Many of the techniques in use have been made much easier for the trained investigators by the proliferation of recordkeeping in our increasingly bureaucratic society.

Recordkeeping itself is becoming fantastically more efficient in reducing space and promoting speedy retrieval of information. We

have moved from the use of bulky folders devoted to individuals to coded file cards, thence to punch cards that can be machine sorted, then to the tape used in electronic memory banks. And now the experts are learning that it is feasible to hook up a number of electronic memory banks, data banks, to one giant system which can be activated for purposes of inserting or retrieving information from numerous locations.

Records on individual Americans now number in the billions. We leave a trail of records behind us from the moment of birth. Our birth, incidentally, is recorded not only on a birth certificate, but also on our parent's income tax return when we became a deductible item.

Consider for a moment this trail of records most of us leave. Non-Government filekeepers have, for example, the information on our income, worth of home, debts, and location of our bank which we often surrender when we apply for credit. Then there are the reports made to insurance companies investigating us as risks. This may involve an appraisal of our social life and our sex life as well as our financial stability. There are the employment files that may be complete with results of personality inventories and lie detector tests. There are hospital and medical records, and the records of the moving companies that have prudently made an inventory of our possessions being moved.

Units of our State and local governments have our school records including our grades, IQ, and any reports of emotional difficulties. At least one of them will have our driving record, any brushes with the law, our property holdings and all licenses obtained, including any for marriage or its dissolution.

The Federal Government has our tax returns over a number of years, our responses to the increasingly lengthy census questionnaires, our social security record, our application for a passport, and perhaps our fingerprints. If we have been in military service, worked for a defense contractor or for the Federal Government, there are lengthy files on us that may well indicate known associates, affiliations, religious beliefs. If we have applied for an FHA loan on a home there will usually be an estimate of the prospects that our marriage will hold together.

These are just a few of the records we leave behind. Many of the filekeepers have been quick to learn that the records they control may hold considerable interest for people outside their own organization. Years after our birth, for example, an interested party such as a lawyer may be happy to pay \$50 for information from our birth certificate, which officially is confidential information. And in a number of cities there are entrepreneurs happy to obtain and sell the information, as well as hospital records, police records, immigration records, passport records, and so on.

Then there are the legitimate organizations engaged in selling personal information about us. The credit bureaus circulate to members the information that we give a store when we seek credit; and if there is any interest the same information may be passed on to curious Federal investigative agencies that inquire. Also there are the giant investigating enterprises such as the Retail Credit Co. which has openly assured prospective clients that it can strengthen any report it makes by drawing from its vast file of investigations made

in previous investigations. The investigative firms making reports for insurance companies on insurance applicants have often felt free to sell the same information to noninsurance clients.

Within the Federal Government agencies have increasingly been developing systematic patterns for exchanging information. When a Federal agent makes a national agency check on a person, it customarily involves checking the files of at least eight Federal agencies.

The individual citizen who is concerned about the erosion of his privacy has up until now had some consolation in the knowledge that all these files about his life have been widely dispersed and often difficult to get at. Digging up a sizable file of any individual has been a time-consuming, expensive proposition.

This is changing with the advent of giant computers with their capacity for instant recall of a great variety of available information. The Federal Government has led the way in installing larger and more sophisticated computers. It has purchased many thousands of computers, including some of the world's largest, and the Civil Service Commission is now operating a training center which has taught 2,300 Federal employees how to get maximum usable information out of various computer systems. The Internal Revenue Service's massive investment in computers to store and assess information on taxpayers is well advertised. We can all be cheered by the promised increase in fairness and efficiency in tax collecting that presumably will result, but if we look forward into the future a decade, the prospect is disquieting. For each taxpayer there presumably can be developed in the electronic memory banks a "cum" or cumulative file covering up to 10 years of his life. Not only would a vast amount of information he has provided about himself and his family over the decade be subject to virtually instant retrieval, but also, theoretically, information about known associates during the period and people and organizations who have had business dealings with him. In short, there will be the capacity, at least, for an instant dredging of one's dimly remembered personal affairs of the past. Unless procedures are developed to prevent unreasonable harassment through this capacity, then the taxpayer of 1976 may well be in a poor mood to celebrate the bicentennial of the Declaration of Independence.

Which brings us to the proposal to consolidate some of the major Federal filing systems into one vast central data bank "by using the new information technology now available." Consultants have urged this concept of centralizing data upon the Bureau of the Budget. A special task force has now been appointed to study the idea. At first this central storage center would pool information now in the files of 20 different Federal agencies. The agencies were not specified in the announcement creating the task force but the pooling reportedly will include records from the Internal Revenue Service, the Census Bureau, the Bureau of Old-Age and Survivors Insurance, and the Federal Reserve Board, to mention just four. Presumably in future years more and more agencies—and more and more of their records—would enter the pool.

The announcement implies the Government is interested only in assembling statistics in more readily available form. But every one of us in this room is a statistic, especially if the statistic involving us has our social security number attached. One consultant to the Bureau of

the Budget has been quoted in the Washington Post as urging that valuable information is lost if confidences are kept and statistics are made anonymous too early in the game. No secrets would be kept from the central data center. The raw data about people's lives would be fed into the central computers without concern for confidentiality and the computers would be programmed to act as the censors. If the Government is sincere in saying it is interested only in generalized statistics, then it would seem essential that all individual identification of a statistic be removed before the kernel of desired information is fed to any central computer system.

But apparently more than one central data center is envisioned, and at least one would deal with live people, not depersonalized statistics. In the Saturday Review of this past week John W. Macy, Jr., Chairman of the U.S. Civil Service Commission, details in glowing terms the wonders of "Automated Government." In talking of the Federal Government's monumental job in keeping track of all its employees, he proposes that—

We must have integrated information systems. This will require the use of information across departmental boundaries * * * Direct tape-to-tape feeding of data from one department to another may become common.

He and others talk of the great gains to come from centralizing data about millions of people in or out of government. There would be the broadening of the horizons of knowledge, the greater efficiency, the dollars saved.

We should be wary of promises that the goals of such consolidation of data are only modest ones that would interest statisticians and planners. Unless there are safeguards, pressures will surely grow to assemble more and more specific data about specific individuals. When the social security program began we were assured that our social security number would be guarded as a secret so that no one could possibly use it to keep track of our movements. Today we must write our social security number not only on our income tax return, but must supply it to banks holding our money and to organizations making payments to us. Our social security number in fact is so easily obtainable that one nationwide investigating firm has a line on its standard form where the investigator must list the social security number of the person he has investigated.

Or consider the census. The authors of the U.S. Constitution called for an "enumeration" of the population every 10 years. But by 1960 the census has gone far beyond enumeration. Many millions of citizens in 1960 had to answer 165 questions about their lives, purchasing habits and incomes. And the pressure is growing to add a host of new inquiries such as ethnic origins, religious affiliation, schooling, et cetera, to the 1970 census. Failure to answer every question the census director decides to ask you can result in a fine or jail sentence.

We should also be concerned about what seems to be a lack of sensitivity among some administrative officials about the implications to the individual involved of becoming computerized by the Federal Government. The announcement of the creation of the task force detailed several points to be studied but no mention was made of exploring the impact on the citizen. And Mr. Macy in his enthusiastic descriptions of automating the Federal processing of personnel, said that the Government must ask: "What parts of the job can a com-

puter do better—and which parts can men do better.” He is presumably influenced by the per-dollar performance criterion so popular now in Washington.

In all these plans for centralizing data about citizens it seems to me that the crucial question is whether we are letting technology get out of hand without being sufficiently concerned about human values.

There would seem to be a number of hazards in the growing fascination of the Government's electronic file keepers with the idea of exchanging and pooling data on the lives of our citizens.

First, I believe the concept of having a central data bank for use in making decisions involving citizens threatens to encourage a depersonalization of the American way of life. Our people increasingly, and rightly, are resenting their treatment as numbers being controlled by a computer. This resentment is believed to be a factor in the student unrest at the vast State universities, where the student's exams may be machine-graded and his ID number is often printed twice as large as his name.

As for the management of Government personnel by one super-machine, it should be noted that even the best of machines cannot assess the unique personality, the special talents, the particular aspirations and motivations of the individual citizen. And all the recent evidence indicates that any normal citizen performs best where he is encouraged to take personal responsibility for handling a special task in his own unique way.

Mr. Macy is pleased to report that in our automated Government hundreds of thousands of people already are being largely hired by machine. The applicant makes marks on paper in a form that can be digested by the computer. The machine grades him, decides what the passing grade will be for any particular batch of applicants, and then writes a letter advising each applicant if he has passed or failed. I am reminded of a description given me of some of the new automated food canneries. A truck brings baskets of peaches up to the automated building. Once the peaches are unloaded automated machinery takes over. The peaches are washed, peeled, sliced, pitted, siruped, canned, packed in cartons entirely by machine. The cartons, properly labeled and consigned, emerge out the other end of the building.

Most of us applaud the automated processing of peaches. But does it follow that we should applaud the automated processing of people? I think not.

A second obvious hazard inherent in the central data banks is that they will increase the distrust of the citizens in their own Government and alienate them from it. People are becoming wary of what they tell their Government as they discover that information they are confiding for one purpose may be used to affect their life in some entirely different connection. If what they tell the FHA to get a home loan turns up as a knockout factor when they seek a job with a Government contractor, they will start being wary. And they will warn their friends to be wary.

In addition there will inevitably be a suffocating sense of surveillance as the public learns that their Government is developing an all-seeing eye. In the past, one of the hallmarks of totalitarianism, whatever its particular form, has been this sense that somewhere there is an all-seeing eye.

A third hazard inherent in the central data banks is that they will greatly increase the likelihood that the life chances of many citizens will be unfairly affected. A central file can absorb large batches of data about people but it is ill equipped to correct errors, allow for extenuating circumstances, or bring facts up to date. An acquaintance related to me his wrath when he discovered, quite by accident, that his local credit bureau, in a litigation report on him, listed him as having been the target of three lawsuits for failure to meet commitments. On the record he obviously was a person to beware.

The facts were that the first was a \$5 scare suit back in the 1930's over a magazine subscription he had never ordered. Nothing came of it. The second involved a disagreement over a \$200 lawyer's fee. It was later compromised amicably and withdrawn. The third involved a disagreement with a client over a fee he had charged, for services rendered. This was the only one of the three that actually got to court and he had won it. It took the man 2 days of digging to clear his record by proving to the bureau's filekeepers the disposition of the three suits.

Many employers including the Federal Government require a job applicant to note if he has ever been held by a law-enforcement agency for investigation. In recent years hundreds of thousands of citizens have been held momentarily for investigation and then released with no charges made. It is hard to explain to a computer feeder the innocent circumstances.

Even more serious in affecting one's life chances is the fact that the computer is incapable of making allowances for early errors or indiscretions. It has no capacity to recognize that people indeed often do change and become more responsible as they grow up. The son of a friend in a Midwestern city applied at several department stores in the area for a job when he was graduated from high school at the age of 18. He had recommendations from his minister, Scoutmaster, high school principal, and chief of police. But no store would even give his application serious consideration. It turned out that his name was in a central file maintained for the stores, possibly a computerized one, of known lawbreakers. Five years earlier, at the age of 13, the boy, while still figuratively in short pants, had been caught snitching \$2 worth of fishline from a store.

America's frontiers were largely settled by people seeking to make a fresh start. They were often seeking to get away from something unpleasant in their past, either painful episodes, misdemeanors, poverty, or oppression. Today with episodes of our past increasingly being recorded in central files and computers the possibility of the fresh start is becoming increasingly difficult. The Christian notion of the possibility of redemption is incomprehensible to the computer.

Finally there is the hazard of permitting so much power to rest in the hands of the people in a position to push computer buttons. When the details of our lives are fed into the central computer where they are instantly retrievable, we all to some extent fall under the control of the machine's managers. Public figures running for office in opposition to allies of the machine's managers possibly could be smeared with information from the computer at a point where there is inadequate time to set the record straight. In recent years we have seen at least one notable case in Washington where information from

a secret dossier was used to try to intimidate or discredit a person who was making statements embarrassing to certain high officials. The filekeepers of Washington have derogatory information of one sort or another on literally millions of citizens. The more such files are fed into central files, the greater the hazard the information will become enormously tempting to use as a form of control.

Some highly knowledgeable people have been issuing warnings about the hazards residing in exploitation of the computer. These are the computer designers themselves. One computer maker, Bernard S. Benson, has conceded that the concentration of power in the form of accumulated information can be "catastrophically dangerous." And at a meeting of computer experts sponsored by New York University, another expert, computer scientist Eldridge Adams, said that the electronic computer systems being used by Government agencies were collecting so much information about families and individuals that those who controlled the machines were achieving a "truly frightening" power. He said that without proper control the computers could convert our society into the Big Brother regime predicted in the book "1984."

Let us remember, 1984, is only 18 years away. My own hunch is that Big Brother, if he ever comes to these United States, may turn out to be not a greedy power seeker, but rather a relentless bureaucrat obsessed with efficiency. And he, more than the simple power seeker, could lead us to that ultimate of horrors, a humanity in chains of plastic tape.

I would hope that this committee, by its power to influence governmental procedures and to propose legislative safeguards—and the Congress, by its power to legislate and to exercise oversight—will take action promptly to assure that such a state can never come to pass in this land.

Thank you very much.

Mr. GALLAGHER. Thank you very much, Mr. Packard, for your statement which gets to the heart of the fears that many of us have as we view the escalation of efficiency and economy that is always possible and probable in looking down the road of computer progress.

The real problem is not that a computerized data bank can be created. I think all of us agree that it can. There are some reasons why it should.

What this committee is seeking is suggestions you might offer as to how safeguards—as to what safeguards—can be installed in the computer process.

I am not satisfied in my own mind that such safeguards can be properly built in, but if they can be installed, certainly I would suggest as

Mr. PACKARD. If they can be installed, certainly I would suggest as a minimum that they must be. I think that the Congress should, in its functioning as a watchdog of the executive arm of the Government, make sure that information does not leave one department to go into a central file until individual identification is removed. How this would be involved in Mr. Macy's proposal to make one vast Federal file of Government employees, I do not know. The only heartening thing about his proposal is that it does not involve all American citizens; it simply involves the millions who are involved in the Federal Government.

But even in his case, I think it is urgent that this committee look into the proposition very carefully and look into the possibilities of safeguards in terms of information being passed from one department to another on what he calls a tape-to-tape basis, across departmental lines.

Mr. GALLAGHER. Is it your feeling then that any central data bank should confine itself to statistics that are sanitized of individual identification?

Mr. PACKARD. That is certainly correct, sir, yes.

As I understand the technical problems, this would be a little more expensive, but certainly if the Government wants to get into assembling statistics that can be used by the Government's planners in terms of our larger scale programs, I think that individual identification must be removed and I don't think the Government should be involved in pooling information where such information cannot be removed—where the identification cannot be removed.

Mr. GALLAGHER. Of course, this is one of the problems, as we view it—the hearings are just beginning—the more safeguards that you attempt to build in, the higher the cost becomes.

Therefore, what we fear is a quick and dirty computer—quick and dirty in the line that it would be a system quickly put together and not free of the safeguards, or rather, not having the safeguards that are so necessary to protect the citizen.

It is my understanding in the computers we use for defense, the most expensive part of it becomes the safeguards that are necessary to be installed, both from a hardware standpoint and a software standpoint, and that when you get into this area you increase the cost from 3 to 10 times the cost of the system itself, but herein lies the danger.

What would your comment be as far as the central data bank or the credit collection system or the files that now rest in the Government are concerned, as to a law that might allow an individual citizen to have access to that information which pertains to him? Therefore, he could check it for accuracy and this would keep the system a little more honest.

Mr. PACKARD. I was greatly impressed by this suggestion when you first made it. I think it is an excellent proposal. I think also that if it is inaugurated, the individual citizen should be provided information on how he can make the check without going through a maddening runaround in Government bureaus to try to get information.

I have to give my social security number to many different organizations now and I am a little obscure on what my number really is, although I have been using it for many years, so I wrote to social security asking for a confirmation. This was more than a month ago and I still haven't gotten any word. I don't quite know how to go about it. I simply wrote to Baltimore and that is as far as I know.

Mr. GALLAGHER. Mr. Packard, you cite some hair-raising facts and statistics in your book, "The Naked Society," concerning the compilation of statistics and dossiers on millions of Americans in the Federal Government. Your citations include the exchange of information by Government bodies that possess confidential records and the swapping of information between Government file builders.

This committee has had considerable examples that have been cited where there was a free and easy exchange of information—lie detector evaluation, psychological test results—between personnel officers.

Have you any more recent information in this area and could you explain what implications they may have in connection with the proposed centralization of these dossiers in the Federal Government?

Mr. PACKARD. I have a great deal more recent information that does not spring readily to mind in organized form. Certainly it is true, as you indicate, that the results of lie detector tests have been passed around, and I know at some of the credit bureaus there are regular desks where Federal agents can come and take information from the credit bureau forms.

You also have, of course, the exchange of information on criminal activities among about eight different Federal agencies involved in having any information about crime. I suppose we should applaud this where you are dealing with known criminals, although I think they also exchange information about suspected criminals. Perhaps this is defensible as one of the areas in this computerizing and centralizing of information.

In general, when you are dealing with the citizen as a free citizen, I think he is entitled to know the information he gives to one arm of the Government is not going to be used against him by another arm of the Government when he assumes the information was given confidentially.

Mr. GALLAGHER. You have mentioned the inherent fear of our citizen. This may well be a cause for the unrest that prevails in our country today. The specter of a human being coping with a fellow human being is not insurmountable, but now that he is overawed because he must now cope with a machine plus a human being, perhaps this awe is justified, but is this justification, in your opinion, something that we must accept, or is it possible for the man of the future to cope with a machine which will control his destiny?

Mr. PACKARD. I think that is the fundamental question, Mr. Chairman. I do not think the answer must necessarily be a negative one. I think Aldous Huxley before he died said that just because there are blind forces at work on the lives of individuals, this does not necessarily mean the individual cannot protect himself. I think all of us as Americans and as individuals—and this includes members of the Government and Members of the Congress and citizens and individuals—need to be aware of the fact that we do have the blind force of the computerized age that we must cope with, and we must put boundaries around it so it will serve us usefully rather than become a tyrant.

Mr. GALLAGHER. Dr. Westin, an expert on the problems of privacy, says:

Unless the issue of privacy is in the forefront of the planning and administration of future computer systems, the possibilities of data surveillance over the individual in 1984 could be chilling.

Would you care to comment on this?

Mr. PACKARD. I certainly would agree that is correct. Your earlier comment about the awe of computers I think is important, because people are more frightened of things they cannot understand, and I cannot understand the computer myself. I have been through the IBM factory and have had it explained to me and I have talked to

many computer experts, but I would not have any assurance that I know what it is all about, it is changing so rapidly and so swiftly. I think we do have this threat, as Dr. Westin said and as many others have said, hanging over us that the machine can dominate our lives.

Mr. GALLAGHER. There is a certain mystique that the computer experts have created that all will be well if we just leave it in their hands and that we are creating a "we" and "they" society, "we" being the statistics and "they" being those who will see that all is well.

One of the things that this committee is attempting to ferret out is whether or not there is a mystique and whether or not we should trust and rely on this mystique or whether or not it is time that we start taking a hard look at just what the position of the law is, what the position of the citizen is, in relation to what is now a very definite possibility of a central data bank, that central data bank being the step in the door toward the possibility of a personal dossier on all of our citizens in the record collection you have outlined.

Mr. PACKARD. I think it would be ideal if the committee can have the guidance of computer experts who are not associated with organizations that have a vested interest in selling computers to the Government or, in fact, selling computers anywhere. Those experts are at the universities, and I think they could be very helpful.

Mr. GALLAGHER. Mr. Horton.

Mr. HORTON. Thank you, Mr. Chairman.

Mr. Packard, I think there are two things that stand out in your testimony. The first is the detailing of the information that is already available to the Federal Government and other agencies about private citizens. Then the second aspect is that even without the computer there has been a trend away from the confidentiality of information the Federal Government has obtained about citizens.

You spoke with regard to the social security number and the magnification of the loss of private rights there. I think these two points you underscore in your statement are very helpful to the committee.

I think also you have pointed out in your statement that up to this date, at least, there has been a dispersal of this information which in and of itself has tended to give some protection to the individual.

I think one of the big problems we have in this whole area is to comprehend what these computers can do. Would you like to make any comment with regard to that, based on your experience and your study?

Mr. PACKARD. Thank you, Mr. Horton. As I understand it, you will be having further experts on computers who can speak more authoritatively on the capacity of the computer as of July 1966. The capacity of the computers is changing not just by years but by months. I would hesitate to make any comment beyond the fact of what the computer experts themselves are saying, that we are progressing not only from getting information on individuals, but building giant systems—to me this is the fascinating or the frightening thing—giant systems where information can be either put in or retrieved from a number of different locations, including distant ones and even including telephoning information into the computer or calling and getting information by telephone out of the computer. This, I think, is probably the most frightening thing of all in terms of getting the control of the computer out of hand and getting more and more people having

access to the information so security does obviously become more difficult to maintain. If you have a lot of people who can get into the computer and take out information, it always will be harder for any investigating body later to try to trace down how the leak occurred.

Mr. HORTON. I was not so much interested in having you comment on the technology of the computers because I realize that is something the experts will have to do. I was thinking more in terms of your opinion as one who has delved to a great extent into this problem of the invasion of the right of privacy, your comment on how you as a layman, not an expert in the technology of computers, envision what will be happening to the individual citizen with the use of this computer system.

For example, consider how many 12-digit numbers can be added in 20 seconds. With a pencil, the answer is two. With an adding machine, 10. With a computer, 160 million. The rate of change is astronomical. This change is on us already. It is here.

I was more interested in your layman's view as to what is going to happen to the individual with the use of this type of highly technical information or tool which can compile this information and have it available. I was more interested in your personal opinion, rather than the technical aspects of it.

Mr. PACKARD. Certainly there are many functions in our society that can be greatly improved by the use of computers. As a matter of fact, I am using a computer myself in terms of some research I am getting together to work out correlations and findings. So, I do not think we should be frightened by the computer as a machine, but I think we should be frightened by what it can do if the information involves individuals and their identity, and I think we need to make sure that before the Federal Government gets too deeply involved in installing computers that have data fed into them involving individuals' records, that this body and the Congress make sure that the individual identification is removed from the material.

Mr. HORTON. You would not, certainly, curtail the population information about people?

Mr. PACKARD. No; certainly not.

Mr. HORTON. You are not advocating that computers not be used.

Mr. PACKARD. Oh, certainly not; no.

Mr. HORTON. You are advocating that this technological advance be harnessed and that there be established safeguards to protect the individual.

Mr. PACKARD. That is correct.

Mr. HORTON. One of the proposals or suggestions which you would make would be along the lines of that which the chairman has made, to give some sort of right to the individual to know what information is available on him so he can correct it or have his own opportunity to be heard, as it were.

Mr. PACKARD. That is correct, yes.

Mr. HORTON. Have you any other thoughts with regard to how this advance could be harnessed and safeguards built into it?

Mr. PACKARD. No thoughts occur to me offhand, no.

Mr. HORTON. Have you any thoughts or any possible recommendations with regard to how the Congress could act in this field?

Mr. PACKARD. I think the Congress and this committee and several of the congressional committees have been extremely effective in their

roles of alerting, simply by making Federal agency directors aware of the human implications of what they are doing, as, for example, the success which has been achieved in persuading the various departments to make less use of lie detectors and less use of personality testing, the post office to stop using the mail cover, the Justice Department to stop using wiretapping, and many agencies to stop using the snooper buttons. All these have come about not by legislation but by the mere fact that a body such as yours has explored the situation and made the administrators in the various Federal agencies aware, perhaps for the first time, that there are human value issues involved, and this is what they have been doing, and that they have usually responded by establishing safeguards.

Mr. HORTON. Thus, you feel the action of committees having hearings such as this focusing attention on the problem will have some benefit?

Mr. PACKARD. I certainly do, yes, sir.

Mr. HORTON. You referred to Mr. Macy's comments in an article in the Saturday Review. What was your reaction to this? Do you feel the Government is going too far in this automated process in regard to civil service?

Mr. PACKARD. I think Mr. Macy is a fine man but—

Mr. HORTON. I am not talking about him personally.

Mr. PACKARD. I think he is overly fascinated with the wonders of electronics in terms of reducing the cost of sorting personnel and processing personnel. Since the Federal Government is involved in dealing with millions of people, he sees it in terms of millions, and dollar costs per unit. I think from the standpoint of all that is being learned by the behavioral scientists on human motivation and what makes people perform better, people perform better if they are given a chance to perform in a unique way, and also they perform best if they have a sense that they are being trusted. When people have a feeling that they are not being trusted, they tend indeed to become more untrustworthy. This is what I think you had. The agencies that were using the lie detectors and similar things were simply digging the holes deeper because they were making people more untrustworthy by that fact.

Mr. HORTON. Another point you indicated earlier was the removal, if possible, of the individual identification. It seems to me this would be difficult to accomplish, or else the information would not be beneficial to the Federal Government. It seems it is an impractical possibility.

Mr. PACKARD. AS I understand it, the Bureau of the Budget has proposed the central data bank for reasons of overall planning, rather than for information about individuals. Ostensibly, there would be no gain to the Bureau of the Census in having the names attached to all this information it is getting. The problem is apparently it would be difficult to wash out this information from the tapes if it were fed into a central computer. That is the heart of the problem, I believe.

Mr. HORTON. That is all the questions I have, Mr. Chairman.

Mr. GALLAGHER. Thank you, Mr. Horton.

I agree that is the heart of the problem, and that is what we are trying to spotlight today—the necessity of eliminating the individual name if we are interested merely in statistics for problems of planning.

If this were not one of the safeguards and names and social security numbers remained on the tapes, do you see a real threat here, or are we getting prematurely overheated in our concern?

Mr. PACKARD. I do not think you are getting prematurely overheated at all. I think we should all be scared stiff about the possibility that these giant machines would be fed data about individual Americans and that this information would be retrievable by a number of different organizations or groups. I think this would clearly create the preconditions for a totalitarian system.

Mr. GALLAGHER. Looking down the path, assuming we get beyond 1984, is it not one of the great responsibilities of our Government to guarantee and protect human values, and is it not necessary at this point to start programing our own Government toward this end?

Mr. PACKARD. I certainly agree, yes. I think any government that has control over a people has at the minimum a responsibility to treat all individuals involved with a sense of decency and dignity. I do not think you would have this sense of decency and dignity if we are treated as numbers in a memory bank and under the control of a giant computer center.

Mr. CORNISH. Mr. Chairman, I have only one question in the interest of time.

Mr. Packard, I was very much interested in the example you gave in your testimony of your friend and his trouble with the credit bureau. I think in answer to one of the chairman's questions you mentioned that in some credit bureaus they actually have separate desks where Federal investigative agents can come in and sit down and make whatever notations they want to.

Mr. PACKARD. Yes.

Mr. CORNISH. We would assume, then, whatever notations they made or whatever copies they made would become, presumably, a part of a Federal file somewhere.

Mr. PACKARD. That is correct, yes.

Mr. CORNISH. If we examine the idea of a personal dossier bank, then it would be a possibility at some time in the distant future that the very information which was obtained from a private credit bureau could end up in a Federal dossier center.

Mr. PACKARD. Very definitely, yes, sir.

Mr. CORNISH. That leads me to ask you this question. Do you think this might be the proper time for the Congress to go back to the original source of the information in the credit bureau and possibly institute some new safeguards affecting credit bureaus? What I am suggesting is perhaps a requirement that an individual be permitted to examine his own credit report on file with the credit bureau to determine its accuracy and completeness.

Mr. PACKARD. I think that would be an excellent idea. I think also it would be very helpful if the Congress did look into the practices of these investigating agencies such as the credit bureaus that accumulate fantastic amounts of data about individual citizens and, in the absence of stiff regulations controlling them, have rather relaxed policies about exchanging information with other people.

Mr. CORNISH. You have devoted some discussion in "The Naked Society" to the credit bureaus and their reports. Would you agree that credit bureau reports are definitely in the stream of interstate commerce?

Mr. PACKARD. That is a very provocative thought, and certainly true because the credit bureaus as a matter of function exchange information in a network all across the country. More than 100 million records are tied in through the exchange of information that is available.

For example, if a man from the State of Nebraska moves to the State of Connecticut and applies to a store in Connecticut for credit, the credit bureau can put in a request for the Nebraska credit rating on him. So this is an interstate operation.

Mr. CORNISH. In your experience, this information does cross State lines?

Mr. PACKARD. Very definitely. Millions of items a year cross State lines; yes, sir.

Mr. CORNISH. Thank you very much.

Mr. GALLAGHER. Mr. Romney.

Mr. ROMNEY. Just one question, Mr. Packard. I think we can see from your statement that you would have reservations about a central personnel data center. Do you actually oppose the concept within the Federal Government of a central personnel data center for Government employees?

Mr. PACKARD. Yes. I think in the announcement that Mr. Macy made, in his enthusiasm he did not put enough emphasis upon the hazards involved in terms of human values and the spread of information. He seemed to assume that every bit of information that any branch of the Government gets on an individual should be pooled. I would have reservations about that, yes, and would view it with considerable concern. I would hope that the committee would do that, too.

Mr. ROMNEY. That is all, Mr. Chairman.

Mr. GALLAGHER. Mr. Forsyth.

Mr. FORSYTH. I am a little confused by some of the mixing of terms and agencies and everything else. It seems as though we are mixing sensitive and insensitive information together, if there is such a distinction. We are also mixing the type of people and agencies that can withdraw information. We are also, I think, mixing up—at least, it seems to me to be confused a bit—whether or not the names are linked to the information.

As I understand it, to go back down the order in reverse, there is no way that a central data system can be effective for a multitude of purposes unless the names are linked to the information at some point in some computer, even though perhaps not in the active set of files or active tape going through the machine; is that correct?

Mr. PACKARD. I do not know. I think if the Bureau of the Budget is sincere in what it says is its aim in developing this central data system, it is not interested in individuals but is interested only in Government broad-scale statistics that can be used.

Mr. FORSYTH. They say that is true, but they say in order to build a system which is responsive to the needs of users being interrogated by a number of different agencies with different questions, the computer has to go back to the basic building block, the individual, in each case, and even though it does not have to identify him by name, it has to identify him by social security number or something so they do not get duplication of material.

For instance, when new material comes in, it has to be related to that particular individual and not his neighbor, and it cannot be re-

ported on twice. So, each time the computer has to verify back the individual and ask a new set of questions. So, even though the operators themselves may not know the name, even though the information relating to that person will never come out under his name but only as a statistic, the system still has to know his name. I believe that is correct, is it not?

Mr. PACKARD. I do not think the whole system would have to know his name. I think the agency contributing the information would need to know his name.

Mr. FORSYTH. By "system," I meant the one main computer.

Mr. PACKARD. No; I do not think so. I think you could have an automatic altering of numbers and setting up a new system of numbers so they would not be tied to the social security number.

For purposes of consolidation, you could assign any individual a number that would not be revealing of anything about him except this would go back to the same building block.

Mr. FORSYTH. Within that computer. Somewhere in the central system, some group of people have to have a code which codes that number to the person.

Mr. PACKARD. It should be the department or agency that supplied the information in the first place. I think you do get the hazard when there is a central knowledge of the individuals.

Mr. FORSYTH. The problem with that is that another agency sends in information, some of which is duplicative and some not. It is fed into a central computer, and if it is set up under a new number, then you have the same number reporting twice, with some duplication. So the same number has to come each time from computer to computer.

Mr. PACKARD. That I think would be the heart of the problem. I do not know the technicalities of it. I think this would be a good point to explore with computer experts rather than with me.

Mr. HORTON. I think one of the points you are trying to make is if there is any way to disperse the information within the computer bank, this at least would be some type of safeguard, just as the dispersal of this information now without computers is somewhat a safeguard to the individual.

Mr. PACKARD. That is correct; yes, sir.

Mr. HORTON. You do not know technically how this can be accomplished.

One other thing I wanted to ask you about. Do you feel there is a basis for the Congress perhaps, or whoever is in control of this system, limiting or having a limit placed on it as to what data can be placed in the bank? Do you see what I mean?

Mr. PACKARD. Yes, I think this should be a concern of this committee. What type of data can be properly and safely put into central data systems should be a concern of this committee.

My own feeling is that you are getting into danger as soon as you get any data that can be identified in terms of an individual citizen or taxpayer.

Mr. HORTON. You made the point with reference to the census, that it was basically, in the beginning, just an enumeration of the population, but now it has gotten into a lot of personal questions. The thought I was trying to follow with you with respect to this is whether

or not we should limit the data and information concerning the individual and use that technique as perhaps a means of safeguarding and controlling.

Mr. PACKARD. I think you are correct. I think you would be safer if you are going to start a filing system that is going to lead to a central filing system, the identifications should be removed at the original agency before the material goes on tape.

Mr. HORTON. Thank you.

Mr. GALLAGHER. Mr. Packard, you hoped the committee would look into Mr. Macy's suggestion that there be computerization and central files on Federal employees. I assure you if such a system is put together, it is our hope and the insistence of this committee that each employee will have access to his own file to see what is in there so that it is accurate and honest. I think this is the only way that an employee would be able to cope with all the information-gathering services so he would be put on notice and would have an opportunity to examine what has been collected on him.

Mr. PACKARD. I think this committee would be performing a very great service if it could persuade the Civil Service Commission to make that safeguard available.

Mr. GALLAGHER. I want to thank you very much for your appearance here this morning, Mr. Packard, for your alerting our country in the past long before many people got to thinking about these problems, for your contribution to the people of this country, and for honoring us here with your presence this morning. Looking down the path, if people read all of your books—I hope they do—and we put this question up to a national referendum, I think there would be some predictable results. We want to thank you very much.

Mr. PACKARD. Thank you, sir.

STATEMENT OF CHARLES A. REICH, PROFESSOR, YALE LAW SCHOOL

Mr. GALLAGHER. The Chair would like to call Prof. Charles A. Reich. In behalf of the committee, we welcome you here this morning, Professor Reich.

Professor Reich is from the Yale Law School. He is an expert on the collection of data on individuals and an expert on the legal implications of the collection of dossiers. We have asked Professor Reich to relate his experience of the past to the new problem of the computer and the possibility of computerized dossiers on citizens and taxpayers in the United States.

Professor Reich, we welcome you; would you please proceed?

Professor REICH. Thank you very much, Mr. Chairman.

I might say that the field I teach in is constitutional law. I will talk today about some of the legal aspects of the proposals that have been made.

I might also say I am here in my own behalf, not on behalf of the law school or Yale University or anybody except myself.

When I began to think about this problem, it occurred to me that everybody is in favor of privacy. I noted that within recent weeks, Time magazine, Saturday Review, Newsweek, and all of my friends said they favored privacy, and I believe that you would be able to get a 100-percent vote out of the American people on the same subject.

The trouble comes in particular instances. The trouble is particular invasions of privacy all too frequently take place because, although we believe in it in general, we are frequently unable to see why a particular invasion should be prohibited. Every time a proposal comes along that would invade privacy in one way or another, there is somebody to say it is necessary, there is somebody to say that the information obtained is very reliable and important, and we have to have it, and there is somebody to say that there is no really important new invasion of rights, that is to say, there is someone who will explain that this does not make a very great new intrusion into the life of the individual.

Thus it is that devices like the lie detector, wiretapping, and eavesdropping are all too frequently a matter of practice because we think or somebody thinks that we have to have the information that can be obtained.

These particular devices have been discussed so much that I thought in talking about privacy today I would like to talk about the proposed Federal data center and use that as the way of talking about this problem of necessity, this problem of whether we have to have this particular invasion, too.

I do not know exactly what is proposed in a Federal data center. I will just have to guess. I will just have to assume that the various kinds of information that the Government now has in many different places and many different bureaus relating to school, relating to employment, relating to the Army, to criminal convictions, recommendations that come in from many sources about a person—that all of that would be centralized somewhere and available to authorized agencies or persons. I do not know who they would be.

Mr. GALLAGHER. If I could narrow the issue, Professor, what is before this committee now for our consideration is a proposal by the executive branch for the establishment of a central data bank that would centralize the information collected by 20 agencies of the Government which now collect and publish information, such as the Census Bureau, Social Security, and many of the other agencies. Many of these are now protected by law as to confidentiality.

Along with the proposal is the warranty, for whatever it is worth, that the law will be adhered to and that there will be a protection of the individual who has given the information.

What is now before this committee and what it is concerned with is that while there are now 20 agencies that collect and publish information, there are many agencies of the Federal Government which collect and do not publish information, and we view this as a foot-in-the-door proposition through which eventually the collectors, but not particularly the publishers of information, will also use it in the interest of efficiency and economy. I think what we are considering here is a new proposition, certainly something new in the Federal Government, a departure from the original right of protection of the individual. That is the issue before the committee.

Professor REICH. Many thanks. I take it we are talking primarily about information that does exist somewhere now, and a proposal to centralize it.

One of the things we have to deal with is the argument that the individual be no worse off after this proposal than before because all the

information exists now. I think that is where I feel like taking off on my own opinion.

MR. GALLAGHER. We hope you will, because that is what we are here to listen to.

Professor REICH. The first thing which seems to me basic about dossiers and the centralization of information is that information gets less reliable the further away it is from the source. I always use this as an axiom, a proposition that I would say is true all the time. Let me give you a college illustration to show what I mean.

When our freshmen come in the college, we have upper-classmen as counselors for them, and the counselors are supposed to show them around and tell them where the laundry is and where to go to find Vassar College, and so forth. It is generally a very helpful thing. Part of their duties as counselors is to write a report on each freshman, which goes in a file. They will say whatever comes into their heads about the freshman, that he is nice, that he is not nice, that he has a chip on his shoulder, whatever they feel is an accurate report. That is something between them and the dean's office at Yale College.

If this information gets into a file and stays there, it slowly changes from a reasonably accurate statement to something that could be a tremendous falsehood, because the freshman counselor disappears and we do not know any more who he is if we want to find him to ask him what he meant. The freshman may change. Perhaps he had a chip on his shoulder the first year, but after he got to like the place he got to be one of the nicest guys around. So, the information may no longer be true except as of the time that it was made. Other people reading this may understand it in other ways.

If that particular record, which serves ordinarily a good purpose, were to survive for 10 or 15 years, were it to become a part of other people's information, it seems to me it would become an untruth by the passage of time and by the distance from the source. Indeed, those who have looked at freshman records many years later are often shocked by the idea that they still exist, and wonder why they have not been destroyed.

That is my basic proposition about the development of inaccuracy, and it is my answer to the idea that this data center would be reliable. I do not think it would be reliable.

Freshman records are only something that happen between freshmen and their counselors. I would like to tell you a little about what happens between me and my students, because this is directly related to the data center. I get—and I am not unusual in this respect—all kinds of questionnaires about my students. I am supposed to fill them out and send them often to private people, but much more often to some Government agency. I take it this is the raw material, or some of it, out of which the computer center would have its supply.

For instance, here is the Department of Health, Education, and Welfare asking me about Student "X" whom I know reasonably well. It asks this kind of question: "How do you rate the applicant's relationships with other people? Consider such things as ability to work and get along with superiors and subordinates." Then it gives you answers. For example, you can check this one: "Mediocre. Wants to do things his own way more often than is desirable. Disliked by some associates. Somewhat lacking in tact. Becomes sullen when criticized.

Tends to react negatively to suggestions." There are other proposed answers all the way from "outstanding" to "poor."

Another question: "How do you rate the applicant's personal adjustment? Consider such things as emotional stability and maturity." Let's again take the mediocre suggested answer: "Inclined to be nervous, irritable, easily annoyed. Inclined to get feelings hurt. Has little insight regarding personal limitations."

My point about this is the same one I made about the freshman. That is, first of all, do I really know what I am talking about when I check these things off? Maybe this fellow was in the day before and was in a bad humor, had a fight with his girl friend, and so he was easily annoyed, nervous and irritable. Maybe the next day he would be a charmer all the way through. Maybe I am mad at him for some reason. Maybe I had a headache the day I checked this thing off. At any rate, this information petrifies a momentary flash reaction on my part. I am assuming I am not malicious, assuming I am a fairminded person trying to do a good job. However fair I try to be, this information goes to the Government and there it is, and no power on earth can change it one iota.

It seems to me if I were a psychiatrist, maybe I would be qualified to answer questions like this, but as a professor of law I do not really know anything about the personal adjustment of my students. I do not really know anything at all about their relationships to other people. I see them in a very special situation in the class, and I am asked to say all kinds of things, good or bad, about subjects that I know nothing whatever about.

If I do not fill these out, somebody somewhere in Washington is going to say, "There must be something to hide. This professor is unwilling to answer these questions."

Just think of the poor student who maybe talked only once in class in the whole year and said something that made him look very nervous. He is a nervous man forever, although that may be the one night in the year that he did not get a good night's sleep, or something else.

So, I am talking about the kind of things that ask for more than we know and then make it into the truth.

The Peace Corps is always after me. The Peace Corps asks for a rating on emotional maturity. Remember, again, I am a teacher. I do not know, I would suppose, very much about emotional maturity, but I am allowed to check things like "Candidate is emotionally unstable, has a history of emotional outbursts, withdrawal, other signs of inability to cope with stress."

I am asked, again, for judgments far outside my ability. I must check something. I have no choice. The student may not know anyone else in school as well as he knows me. I am on the faculty. Whatever I say is there forever.

Again, a Peace Corps rating on relationships with other people. I am allowed to say "Superb." How could I say "Superb"? I do not know how he treats fellow students outside of my presence. "Poor." "Doubtful." "Reasonable to believe candidate will have difficulty working with others." Maybe he has trouble working with me. All I can say is that I must answer, and whatever I say is there.

Mr. HORTON. May I ask the witness to establish the basis on which he gets these questionnaires? Are they sent to you in connection with

job applications, or is this something that comes to you on all students who are in your class?

Professor REICH. Mr. Horton, every student who graduates from law school has to get a job someplace, and nearly every place requires references. In the case of the Government, he must give them the names of those teachers he knows best. So, on all the students I know, I receive from private or public agencies questions which are at the student's behest but, nevertheless, he is required to give references. He probably chooses me because he knows me and he hopes I will say something nice about him. Sometimes a student comes in and says, "You don't remember me, but you gave me an 'A' and I would like a recommendation." I say, "Did I? Well, you must be a good student."

You see, I do not even know all the people that well, but the system requires that I appear to. It is in connection with employment that this crosses my desk.

Mr. GALLAGHER. I am sympathetic with the problem, Professor, because we get the same questions as Congressmen, and the only related incident and the whole reason we are asked to serve as references is the fact that a mother or father might have voted for us. We have to fill out the whole business concerning character.

Please continue.

Professor REICH. I want to illustrate this one more time by the Navy, which gives you a series of boxes to check. As to each thing you can say "outstanding," "excellent," "good," "satisfactory," "unsatisfactory." For example, "Ability to lead others," "Degree of cooperation with others," "Emotional characteristics and stability," "Attitude toward carrying out desires of those in authority over him."

Look at the danger of that question, for example. I am in authority over these students. Maybe I am awfully unreasonable. Maybe once in a while they say, "I don't think this ought to be done the way you say. I have a better idea how to write this paper." Is that something that is going to get my back up and am I going to check him "poor" on this?

The point is, if somebody wants to come and talk to me about a student, inside of 10 minutes they get an idea of what I am like and they get an idea of the way in which I talk about people. But a machine does not know those things. So when I say "unsatisfactory" because the man talked back to me, the machine only knows that this man is unsatisfactory. It does not know anything about me. Maybe it is I that is unsatisfactory and not the student. All of that is part of this whole problem. There is no way to go back to the source.

Another source of information that gets into the files is something I would call private adjudications, that is, formal decisions about people that are made outside of the courts. For example, we, the Yale Law School, find that a student cheated and that becomes part of his permanent record. The problem there is to know whether we did as good a job as we should have to find out if it was true that he cheated. We pride ourselves, because we are a law school, on being very careful. We hear the student. We give him every opportunity to explain. We try to find the facts as lawyers should. But schools all over the United States engage in the process of disciplining students, and not all of them are lawyers and not all of them know how to do things fairly. Some of them do not hear the student at all.

Again, what validity do these private decisions have? They can be a curse on the individual for the rest of his life, but you may not have any idea whether they are really accurate or not. They may meet no standards of fairness with which we are familiar.

So, in each case of information other than the formal decisions of courts, we do not know what is really meant by the information in the files. As it gets step by step farther away in distance and further away in time from the original source, it becomes less and less accurate until what was the truth can become a lie.

About people in Government, about workers in Government—I do not want to use the word “bureaucrats” because it is a bad word—I would just like to say when anybody who works in a great organization receives information from a computer center and it says “unsatisfactory” in this category, “unreliable” in that category, it takes a lot of courage for a Government employee to say, “I am going to hire him anyway. I am going to disregard this. I think he looks good to me. I have seen him. I don’t care what this professor said in New Haven.”

Most people in Government, because it is so big, because they are part of a great chain of responsibility, are going to say, “I don’t want to take a chance.” That is the common reaction of a man in a big organization. So when they see something bad, they are going to say, “I don’t trust my own judgment. I had better trust what is on paper, because if we hire this young student, whom we like, and he does something wrong, he turns out to be a loser after a while, it will be my fault. I saw this in the record and I failed to stop it. I am going to be blamed. The safe thing is just to say ‘No,’ and hire a man with an unblemished record.”

So, every normal human reaction is going to be to give more weight to these things in the file than I as the maker of the file ever meant. Often I might check something off and I would like to say to the man who is going to hire this fellow, “Disregard this. We didn’t get along, the two of us. I would give him a chance if I were you.” But I never get to say that.

So the reaction of the normal person who reads the file is to say, “I don’t want to take a chance.”

I have examples, also, of the inquiries that come at the other end. They do not happen to be from Government because I have no access to Government inquiries, but these are inquiries from private people to the Yale file. For example, let us imagine that Yale has its own computer center. It does not. It just has a file. Somebody writes in to the dean and says, “The person whose name appears above has applied to us for a position. We would like any information regarding his scholastic standing, character, and personal habits. Your reply will be kept in strictest confidence.” This comes from businesses, and so forth. This is what I imagine would be the inquiry to the computer center.

Notice that they want anything of a pertinent nature about the personal habits, and so forth. When it comes to Yale, what happens? Well, the dean is not going to answer all these letters. They have a student often, maybe a third-year law student or somebody like that, who does part-time work in that bureau. All he does is go and look at the files of the applicant and pull out anything that he thinks these people

would like to know. So, there is no more control, even at a good university, over this sort of thing than just the judgment of a person in a clerical role who can go and look at all these data and send it forth.

Likewise, it seems to me, the tendency would be for a sort of automatic dispersal of information without any judgment being made as to its quality, because even at Yale we do not judge its quality. If we send it out we just say, "This is in the file, and we suppose this is what you would like to know."

So it is that what one puts in comes out, but it does not come out the same as what was put in.

That is the situation, as I see it, of the data center. The question is: How does this stand with respect to law? How does it stand with respect to the Constitution?

At the very beginning of my thoughts about the law, it seems clear to me that any time bad information is supplied about an individual, his legal rights are invaded at that moment. We have a great common law tradition that defamation of character is a wrong in the law. It seems to me absolutely clear as a starting proposition that anybody who supplies derogatory information about somebody else invades his legal rights. He may have no remedy. That is something that happens in the law. But the beginning of my thinking is that a person has a right not to be defamed, whether it is by a machine or by a person.

The second thing that seems to me so crucial here is that this whole process is secret. The individual does not know what I have said about him. He does not know what is in the computer's file. He does not know what the computer says about him. He does not know what judgments people make on the basis of that.

I think this is a denial of the constitutional right to confront, the constitutional right to face those who make statements about you, to question them, and to rebut, to answer. It is elementary, it seems to me, that this right is lost in the kind of case that I have given.

Suppose for some unfortunate reason I have a grudge against a student and, receiving one of these things, I check "unsatisfactory," and so on; the story, if it came out, would be a very different story if he were able to cross-examine me. He could show there was some bad blood between us or something else, and I was not being wholly accurate. The truth, as lawyers know, is brought out in an atmosphere of adversary proceedings, of cross-examination, of being able to answer, to rebut.

Here we have what seems to me over and over again instances of condemnation without trial, of information supplied without confrontation, and of a denial to the individual of any chance whatever to answer.

The Supreme Court has recently been extraordinarily scrupulous with respect to the right to have a lawyer and the right to confront in situations where people are charged with crime. The right to have a lawyer and the right to confront in situations where people are charged with crime. The right to have a lawyer, for example, begins now at the very earliest moment of contact in the police station.

Here are people who are not even charged with crime, and yet who may be punished far more severely than the ordinary criminal. Here are people whose opportunity to have jobs, to earn money, whose reputations and everything else are about to be damaged forever, and they

have no trial, no lawyer, no opportunity to find out anything. It seems to me without question a denial of due process of law to send forth bad information about a person in secret in that way.

It is in this that I see the essence of the evil of the automatic data center. It is in this notion of the petrification; that is, this man is called bad by somebody, hence he is bad forever, and there is nothing he can do about it. There is no remedy in the law.

It seems to me that we deal, when we think about a computer center, with a wrong which the law is unable to make right in any way that we now know. It is a form of damage without a remedy, and it can be a very terrible punishment, indeed, for the individual.

Beyond the invasion of the right not to be defamed is a second, and some people think, a more vague right, the right to privacy itself.

When information about a person of the type I have mentioned is distributed all over to everybody, certainly you could say at the very beginning that there is no privacy. That is, my opinion about a student is a private matter perhaps between me and the person who wants to employ him and I might be willing to talk to an employer about a student, but when that is broadcast all over the Government, given to anonymous people all over, then it becomes a very unprivate affair. So we see there the exposure of the individual, whatever his weaknesses are, to the scrutiny of everybody, so there is this second legal issue about privacy that seems to me fundamental.

Now, the right of privacy is not spelled out in those words in our Constitution and I think there is a reason for that. I think that the reason is in the 18th century, when the Constitution was written, Government was very limited. Government was supposed to do only a few things, minor things we would say today, and I think that the idea of privacy being invaded in the way it can be today never occurred to the people who wrote the Bill of Rights. But everything that did occur to them in the way of invasion of privacy they wrote in. So what you find if you read the Constitution is that in every way in which they understood privacy then, they protected it in the Constitution.

Let me illustrate: They protected speech and expression and beliefs, and those, it seems to me, are illustrations of privacy. They protected religion and conscience, each individual's to be his own. They forbade the quartering of soldiers in houses. They protected the right to bear arms—and there are many other reasons for that, but one of them is the man with his rifle in his home. They protected people against the search of the person or the search of the home without a warrant and in unreasonable circumstances.

They protected people against being forced to incriminate themselves by any official body. They protected people against cruel and unusual punishment, thus in effect protecting the body against invasions that were deemed unreasonable at that time.

When they got through with all the above, they protected all the other rights of the people not enumerated in the Bill of Rights and not specifically handed over to Congress by a particular part of the Constitution.

I say, myself, that that is privacy as they understood it. That is all of the invasions of privacy that they knew of in their time, and had they known of these, it seems to me they would have dealt with them the same way.

Now, all of us know that our Constitution was framed to exist over the ages and thus has always been interpreted to deal with the problems of our times, of the times that occur and it seems to me, therefore, that there is a constitutional right to privacy which does exist and it includes the right not to be defamed by anybody in official position.

I might say there that Justice Brandeis was the author of the famous original article on the right to privacy and he was talking about this very question of defamation, of slander. He was talking, in fact, about newspapers, and whether they could invade privacy and the right which has become established in part as a result of his article back in 1901, which he found in the Constitution, as I find in the Constitution, began with the idea of defamation, the idea that we deal with today.

Well, that really takes me to the question of, is this necessary? That is, do we have to have this? Is this another example of something where we all regret it, but we have to have it anyway? Must we have the data center to save money, to save time or to save the Nation from some danger?

Necessity, I would like to point out, is a relative word. Things are necessary in one time and not necessary in another because necessity involves a balance.

I might tell my dean that I have to have three secretaries and a thick carpet and an office twice as big as I have and I would say that is necessary. "I can tell you why I need each of those secretaries." But the fact is, in our school other things are necessary too; he figures out how necessary and what is needed in other departments.

Necessity is a budget. Necessity involves a choice among things. I tell you I have to be somewhere at such and such a time and if something more important happens, I don't have to be there.

So when they say a data center is necessary, they are saying it would be useful. They are saying, "We could use one." They are saying, "If we had one, it would do the following useful things" and they list them: save money, save time, and so forth. That tells you it would be useful, but it doesn't tell you it would be necessary.

When we decide whether a thing is necessary, we have to figure out the losses. What would be taken away by this proposal?

There, it seems to me, we come to what all of us realize this proposal is going to do something to the character of the American people. The question we have to think about is what is going to happen to the character of the American people and how serious is it?

We have already had mention this morning of the great American idea of "beginning again," starting anew, getting a second chance, and that is something we would lose by this. We would have a situation in which nobody got a second chance, no matter how young, no matter how foolish, no matter how easily explained the circumstances; we would establish a doctrine of no second chance, no forgiveness.

One life, one chance only. That seems to me very different from the American dream.

We would have, in addition to that, a waste of people, a human waste. We have a lot of people in this country but I don't think we can afford to waste them and many people, including some saints, have done wrong early in their life and then lived to be worthwhile people.

Some of the best people are people that did something wrong and then went on in the light of their understanding of those wrong things, to do something right. And I can think of a lot of great people in the world who, if they had been stopped because they once took the wrong path, they would have been lost to us. They would have been some of the greatest religious leaders, some of the greatest political leaders that we have. We ought not to build into a machine anything that will keep us from having the benefit of those who once made a mistake in their lives.

A third thing that we will have, it seems to me with this center, is a nation of people who are afraid. One way I tried to prepare for being a witness here was to talk to people in New Haven. A man in the dry-cleaners listened to the best I could describe the Federal data center and the first thing he said was, "Why, that sounds just like Russia. We are going to have a number instead of a name over here pretty soon and it is not going to be very American."

I said, "You put it very well. Can I quote you?"

He said, "No, I don't want to get into trouble. Don't say a word." Then I thought, there it is. They don't even have the center yet and this man who just works in a drycleaning establishment in New Haven is afraid. He doesn't want his name mentioned to those anonymous people in Washington who might write it down and might make some trouble for him someplace, somewhere.

If we have this center, it seems to me we will increase the number of people who are afraid and we will begin to lose what we like best in the American character, people who are willing to speak up, people who are willing to do things and not look around over their shoulder to see who is looking on.

When I spoke of the Constitution and the right of privacy and the right of confrontation, the right to be present at your own trial, I would like to emphasize that I am speaking of a minimum when I speak of the constitutional law. The Constitution represents not the maximum protection of the individual, but the minimum, and in this day and age in which we have so much pressure to invade the individual's life, I think we shouldn't stop with the Constitution; we should have affirmative laws to protect privacy more than the Constitution does.

It has always been our tradition to pass more laws than the Constitution provides because we know that is only a beginning.

While I think that hearings like this—that awareness of this problem are valuable, I believe in laws. I believe that real protection in this world comes not from people's good intentions but from the law and, therefore, I would like to see some laws on the subject of gathering of information like this.

I would like, in the first place, a law that would prohibit Government agencies from asking some kinds of questions at all. Some questions are either so personal it is nobody's business or so close to the constitutional area of religion and free speech that it is nobody's business in a constitutional sense.

Some information I would say is nobody's business at all. If you don't know that, you just have to hire them without knowing it. It is just too bad, because we don't ask people about their personal lives, in some respects, no matter how much we would like to know.

Now, secondly, I would say that there is some information that may be needed at one particular place. It may be needed for one particular man or agency, but I would say it is to go to no one else. There are other kinds of information that I would restrict only to the place where it was originally needed and I would have it sealed or destroyed when its usefulness had ended. And I would not assume that information that is useful for one purpose ought to be handed out to anybody else for other purposes.

Every time that information is required, I think it has to be justified all over again. It seems to me a very terrible society—and I mean terrible in the sense of frightening and terrifying—where information given to one man becomes information available to all.

I might very well be willing to talk to a Congressman who wanted to hire a confidential assistant, about some student, but I would never talk to the Congressman if I thought he would tell everybody in the world what he had heard from me. So I think you need a law to protect people against that.

I think you need a third law that would see to it that people have a chance to know what has been said about them and to rebut it.

I am constantly being promised by these letters and references I get that everything I say will be kept confidential, kept from the student.

Why am I entitled to that kind of protection, me as a private individual? Why should I be given the privilege of saying what I please about students and not have to account for it?

Now, in my role as a teacher, I have to account for it. If I give a student a bad mark, I have to see him the next day in the hall and I have to say "I'm sorry. You didn't do very good work." I have to face that and I have learned to face it. Sometimes its the person you might like best in the class, you feel quite badly about it, but that is something you have to do.

Why should I be allowed to say something bad about the same student in private and get away with it? I don't see that I am entitled to any such privilege and I don't want that kind of privilege, but every one of these letters assures me that anything I say will never be known to the person involved.

I would like to make the accusers in this situation responsible for what they say and I would like to give the individual a chance to explain, to give his side of the story. That way we won't petrify this information. It seems to me that a proposal like this one for a Federal data center is an example of the process by which government "just happens."

I don't think there are bad people in government who want to destroy the privacy of the individual. I think there are very well-meaning people in government who follow their own jobs out to their logical conclusion and see in this certain advantages for efficiency and so forth, and don't see any more. So a center like this is all too likely just "to happen." It is a very great thing, I think, that this subcommittee is trying to make people stop and think. It is trying to make people, it seems to me, ask themselves, "Is this a proposal we really want, or is this, on the other hand, a rather incredible thing in this country that we should have a proposal to have a file on everybody?"

I guess all that I wanted to say today is simply that we should not permit it to happen. We should have it happen only if we want it to happen. For myself, to those who say that this particular center is necessary, that we have to have this, I would say that what we have to have is a nation of people who are independent and unafraid, and I think that is the only real necessity.

That is the end of my statement. Thank you very much.

Mr. GALLAGHER. Thank you very much, Professor, for your very enlightening statement. It certainly has touched all the bases of our concern.

In behalf of the committee, Professor Reich, we want to thank you for a wonderful contribution to this dialog. I think you have set the basis for some in depth thinking into a problem which disturbs all of us. For your splendid presentation, we are most grateful.

You have touched on many of the things that have concerned this committee in the past. The question of wrong information or bad information becoming institutionalized in Federal dossiers is presently one of the weaknesses of our personnel structure here in Washington. We have had many illustrations of this thing happening now.

The frightening prospect is if this is put into a computer and lasts forever or is made permanent, as you have mentioned.

Only the other day I had a boy graduate from school, an honor graduate, a man about 6 feet 4, who thought he ought to be a Marine officer. It would seem to me he would be the ideal type we want especially since he wants to do his part for the country, being fully qualified physically and academically to be an officer. But shortly before he was to be sworn in, a central traffic data bank turned up the fact that he had 4 parking tickets when he was 17 years of age, and this disqualified him. It showed a certain instability, even though he is now 23 years old and appears to have the right drive to defend his country and get shot at. I do not think that parking tickets ought to be a prohibition to this opportunity.

The frightening part of it was that he subsequently applied to the Navy, who recruited him as officer material, and then it turned up that he was a reject of the Marine Corps and they wanted no part of him.

So you have put your finger on the heart of the problem. We are worried about the dropouts of today, but I am worried about the computer rejects of tomorrow. Within this lies the fact that there will be no opportunity for repentance, rehabilitation, forgive and forget and go on to a happy life, and we are about to change one of the basic and fundamental structures upon which our environment is built.

You have made three suggestions about how we could protect certain taxpayers in the event we get on this path of a central data system. Would you mind outlining those again for the record?

Professor REICH. Surely. Each of these has to be spelled out after hearings, study, and so forth.

First, I think there are questions which nobody has a right to ask any citizen in this country at all—period. I think there are kinds of information that are just plain nobody's business. That is an old-fashioned phrase, but I think it is a good one to remember once in a while. There are just things that are no one's business, and as for those questions, for example, about personal life, habits and ideas, it seems to me we should have a law and eliminate.

To be a little bit more specific, I think we all agree that a question about a person's religious belief is a question that no one in this country has a right to ask anyone else—period. The Constitution says it, but I would like to see the law make it clear to every employing officer in this country as well. That is an easy illustration. Things that go on between a man and his wife and between a man and his children are nobody's business. I think we could think that through and could come up with a list of information. I hardly have to mention it, except that people ask those questions.

Mr. GALLAGHER. You are absolutely correct, because the experience of this subcommittee has demonstrated this has become a way of life, especially with the personality questions proposition that was rapidly becoming a condition precedent to Government employment. Fortunately, through Executive order, we have gotten out, at least temporarily, the questions relating to sex life and private beliefs. I agree with you, perhaps a law is needed, because while Government employees are no longer required to do this, still this exists in private industry and anywhere else that a personality-type question can be asked.

Mr. CORNISH. May I add something at this point, Mr. Chairman?

Professor Reich, if we do enumerate a list of types of questions that cannot be asked or areas which cannot be inquired into, do you not then think there is perhaps an implication that questions outside of these enumerated ones would be all right to ask?

Professor REICH. There is a little danger of that, it is true, except at the end of the law you could say that the listing of these categories here should not be taken to imply that all other questions are authorized. That is done in the Constitution as well. Indeed, the Constitution at the end of the Bill of Rights says the enumeration of certain rights here is not meant to disparage others that are reserved to the people.

Since we are told they now ask everything, it seems to me the danger you suggest is less dangerous than the danger we now confront.

I would like to add to what I just said that I, myself, would not apply the law merely to Government, but I would apply it to those corporations that Congress has power over; namely, those that are in interstate commerce. In other words, I myself think it is just as bad for a private company to do this as for the Government. Congress has power to regulate wages, conditions of employment, and many other things, in these industries, and I think they should regulate this as well if it is now being abused, and I gather it is. So, I would have a law that would be public and private in its application.

I would try to keep the categories somewhat broad in order to avoid the danger you have mentioned.

There is a second kind of law that I had in mind, and that is limiting information to the original purpose intended. It may be that one ought to disclose some aspect of his financial activities to the Internal Revenue Service, but that does not mean that that is relevant to every other person who wants to know about this individual. There are some jobs that are extraordinarily sensitive and confidential in their nature. We do not even have to talk about the area of defense. We can talk about a job in which you are a personal and confidential assistant to a high Government official. Those jobs require some kinds of information that other jobs do not.

So, I have tried to think of the categories of information, of inquiry, and limit the distribution of information once obtained. I think the principle I would have is I would start with the idea that information goes only to the person who is authorized and to no one else, unless there is a specific exception. In other words, my principle would be no distribution beyond the original recipient of information without an exception.

I take it today we have the opposite principle. Distribution is allowed unless there is a prohibition. It seems to me that is the wrong approach.

Mr. HORTON. On this very point, I would like to put into the record at this juncture the article by Mr. Macy in the Saturday Review of July 23, 1966.

(The article referred to follows:)

[From Saturday Review, July 23, 1966]

THE NEW COMPUTERIZED AGE—4: AUTOMATED GOVERNMENT

How Computers Are Being Used in Washington To Streamline Personnel Administration—To the Individual's Benefit

(By John W. Macy, Jr.¹)

In any examination, whether in high school or college or in a civil service written test, it has never been considered cricket to show your paper to anyone else. In these days of automated examinations this same rule may be carried to the ultimate extreme: the only eyes that ever fall upon an applicant's civil service test may be his own. Even though the test may be sent across the continent, graded, and compared with the papers of other competitors, and even though the applicant may be hired and enter upon a lifetime career largely on the basis of this test, nobody but him need see it after he completes it.

This is one aspect of automation that bids to revolutionize personnel management in the Federal Government. Some may regard this feature as depersonalizing. But the truth is that mass examination scoring never was a highly personal activity. The automation of much personnel work of a clerical type may well serve to increase the personal attention managers can give to problems requiring human attention.

Automated examining techniques used by the U.S. Civil Service Commission may be both more advanced and more limited than the general public realizes. During fiscal 1966 the Commission's computer automatically scheduled more than 700,000 applicants into 1,000 examination points throughout the Nation, computed the scores of those who took these nationwide examinations, and notified applicants of the results. On the other hand, these high-volume figures deal only with nationwide written examinations. In many instances, persons who apply for positions are not tested, but rather are evaluated by a team of experts in a specific occupation, and are graded solely on their previous training and experience.

For one of the 700,000 persons who applies for an automated examination, the initial action on his part is simple and easy. He files only a small card form. In due course he receives an admission card, telling him to report at a specified date and hour at an examination point convenient to him. His examination has been scheduled by machine, and the time and location have been printed automatically. In the examination room, the competitor marks his answers to the questions by shading the appropriate block on a set of test-answer sheets. When the sheets are returned to the Commission, computers then take over the next steps. Their output even includes a letter to the competitor notifying him of the test results.

The notification letters roll out of the computer in one long sheet, are mechanically separated, and are finally stuffed into mailing envelopes virtually untouched by human hands. Not only is this process immensely faster, it is more accurate and requires substantially smaller expense than processing by hand.

¹ John W. Macy, Jr., is Chairman of the U.S. Civil Service Commission.

In addition, the computer is programmed to check the validity of test results, to prepare studies showing how different groups of applicants performed on various sections of the examination, and to assist in establishing appropriate passing scores.

Automatic data processing has been applied to personnel management in the Federal Government for only about 6 years, yet the roots of the cybernetic revolution in government extend back to the 1880's. In fact, there is reason to think that the entire development of automatic data processing was initiated by an invention of a young Census Bureau employee appalled by the paperwork of the 1880 tabulation.

Herman Hollerith was a young engineer working on the 1880 census. Seeing a need for something better than handwork on the mass of census statistics, he put together a tabulating machine that he called his "statistical piano." It was somewhat reminiscent of a player piano, in that it used a roll of punched tape to feed instructions into the machine. People who, then as now, condemned the civil service for a lack of imagination and innovation, must have been looking the other way. Even the inventor may not have realized what he was starting, but in the 1890 census Hollerith's device was credited with saving 2 years of work and \$5 million. Later it became the foundation for a phenomenal business—the company now usually referred to by the initials IBM.

The Government also pioneered in the development and use of electronic data processing. One of the first completely electronic computers ever built was called ENIAC, for electronic numerical integrator and calculator. It was produced by the War Department and the University of Pennsylvania, working together in 1946 to solve problems in ballistic research. In 1951 the first commercial computer, UNIVAC I (universal automatic computer), was installed in the Census Bureau, some 3 years before a private company put a UNIVAC into operation. The Government received good value from its investment in UNIVAC I, running up more than 73,000 hours of operational use on the machine before retiring it to the Smithsonian Institution in October 1963.

When first developed, the digital computer was used merely as a large and very fast calculating machine, or for complex accounting and statistical purposes. In Government, priority was given to its employment in the primary mission of the agency by which it was used. By the early 1960's, however, the Department of Agriculture was using computer facilities for centralized personnel management data processing purposes. Its MODE (management objectives with dollars through employees) system is a large-scale centralized personnel recordkeeping and reporting operation, utilizing a computer in New Orleans. In addition to records and reports, the system computes the pay checks for Agriculture's 100,000 employees throughout the Nation.

The Veterans' Administration, with 156,000 employees, was the second large agency to install a centralized, automated personnel system. This system, called PAID (personnel and accounting integrated data system), operates at Hines, Ill. PAID encompasses general personnel management statistics and reports, career development and training records, a file on employees' length of service, payroll information to permit computation of checks by the machine, and information on the authorized number of positions as compared with the number of employees on the rolls. The system also contains a "suspense" file of personnel matters to be brought up on certain dates.

Twenty-two agencies of the Government now have automated personnel systems covering 1,500,000 Federal employees. Systems covering an additional 500,000 are being developed.

The Civil Service Commission first entered this field in administering the Government-wide retirement system. Through an automated procedure, 750,000 retirement accounts are maintained with an annual increase of 45,000 new annuitants.

Three years ago a 5-percent increase in all current annuities was authorized by Congress. This necessitated recomputation of the annuity for every person on the retirement rolls. The last time such a task was required it took months. The added workload was augmented by a stream of letters from Congressmen, justifiably wanting to know why their constituents were not receiving their higher retirement checks, but in 1963, thanks to the wondrous capability of the computer, 630,000 annuities were recomputed in just 10 days and checks started flowing out before complaints and inquiries began pouring in.

The system is now being used to compute deductions for medicare payments for those annuitants who are not receiving social security benefits. A recently

completed management study of retirement and insurance operations indicated that over the next decade more than \$3 million can be saved through further automation.

Increased automation is to be expected. But it is time to ask searching questions about these systems and what they should be doing for us. Automated personnel systems put into use during the past few years are basically record-keeping and reporting systems. But it is a serious mistake to think of personnel offices primarily in terms of records and reports.

Personnel management is principally concerned with finding the best qualified people to fill vacancies, insuring maximum utilization of manpower resources, improving working conditions and thereby improving work—and providing equal employment opportunities to all our citizens, not only at the point of entrance into the service, but through training, promotions, and full career development. Seen from this perspective, automation of personnel operations is just beginning.

As we advance, the question facing us is this: Which parts of the job can a computer do better—and which can men do better? We know that a large part of management is actually clerical decisionmaking, though we have often dignified it in the past with the word "judgment." It requires the identification of relevant facts and the selection of predetermined action on the basis of those facts. This a computer can do beautifully.

In scheduling civil service examinations, for example, our computer makes "decisions" of this kind by the thousands. Why should the time of a man or woman be devoted to such work with less accuracy and little satisfaction? We have other work for men and women, in which they can do a far better job using the huge data resources of the computers. This work involves decisions on personnel planning, the matching of men and jobs, the forecasting of manpower needs, and the important decisions of career-planning.

For proper decisions in these areas we must have integrated information systems. This will require the use of information across departmental boundaries. It is here that current efforts to standardize symbols and codes will pay dividends. Direct tape-to-tape feeding of data from one department to another may become common. These systems will mesh well with developing plans for an executive-level staffing program which will be designed to locate the best possible man for any given top-level assignment, no matter where in government he may be serving.

The computer's ability to search its perfect memory and pick out records of individuals with specific characteristics has been applied in the search for candidates for Presidential appointments. A computerized file containing the names and employment data of some 25,000 persons, all considered likely prospects for federal appointive positions, is searched electronically. This talent bank, with its automated retrieval system, broadens the field of consideration for the President in critical decisions of leadership selection.

Throughout the Government, one of the great responsibilities is to provide true equality of opportunity in employment. To know where we have failed to provide it, where we have succeeded, and how best to plan, we need a multitude of data. Through head counts we know only that a certain number of Negroes, for instance, were on the rolls in certain grades at a certain time in the past, and now we can count that there are fewer or more. But these data do not reveal whether the people in certain jobs came from lower jobs or from outside the Government. They do not assist us in recommending training or evaluating it. They fail to give us the management information required to do a conscientious job of creating conditions that will make a reality of equal opportunity.

To obtain additional and more accurate information, a new effort has been initiated in this area. By means of a voluntary racial designation prepared by employees themselves after employment, reliable information now can be fed into computers where it can be confidentially stored and used.

Most Federal managers need more knowledge of computers in order to best use their capacities. With this in mind the commission last year established an ADP Management Training Center in Washington. More than 2,300 Federal employees have attended its sessions.

There seems no doubt that increasing use of computers in Government, accomplishing many of the clerical tasks by machine, will affect the skill requirements and the "occupational mix" of government service in the future. The Civil Service Commission has made an extensive study of this question, and is giving it continuing attention. Employee displacement has not been extensive; with intelligent planning an agency can prevent hardship for the employees affected.

An outstanding example is furnished by the Internal Revenue Service, which has done an exemplary job of minimizing the impact on employees in its extensive ADP conversion program through advance planning, and intensive retraining and placement efforts. This is the kind of personnel job no computer can handle.

This seems to me to be the answer to those who fear that computers will de-emphasize humanity. Far from it! By removing the clerical decisions and the mass of paperwork details the computer may well free the mind of man for more worthy use.

Already it has heightened the need for imaginative and innovative managers who can grasp ideas, think in broad, philosophical terms, and apply such terms in decisions relating to public welfare. It has forced a finer degree of quantitative precision in executive judgment. It has liberated the manager to give his mind to greater scope of creativity. Rather than degrading the worth of the human being, the computer has placed a premium on man at his best.

Mr. HORTON. On page 25, Mr. Macy in his article says, picking it up and perhaps it may be out of context:

In scheduling Civil Service examinations, for example, our computer makes decisions of this kind by the thousand—

Meaning judgments that are clerical decisions about whether people are qualified or not.

Why should the time of a man or woman be devoted to such work with less accuracy and less satisfaction? We have other work for men and for women in which they can do a far better job using the huge data resources of the computers. This work involves decisions on personnel planning, the matching of men and jobs, the forecasting of manpower needs, and the important decisions for career planning.

On this very point that you were making with regard to stopping the information at a certain level and not letting it get across into other departments, Mr. Macy continues and says:

For proper decisions in these areas we must have integrated information systems. This will require the use of information across departmental boundaries. It is here that current efforts to standardize symbols and codes will pay dividends. Direct tape-to-tape feeding of data from one department to another may become common.

This is Mr. Macy talking with regard to the role that he has as Chairman of the Civil Service Commission.

These systems will mesh well with developing plans for an executive level staffing program which will be designed to locate the best possible man for any given top-level assignment, no matter where in Government he may be serving. The computer's ability to search its perfect memory and pick out records of individuals with specific characteristics has been applied in the search for candidates for Presidential appointments.

This is Mr. Macy saying it already has been used.

Mr. GALLAGHER. Patronage of the computer.

Mr. HORTON. And I think I would rather have the patronage system than this.

A computerized file containing the names and employment data of some 25,000 persons all considered likely prospects for Federal appointive positions, is searched electronically.

This is not what we are going to do 5 years from now, but this is what we are doing now.

This telebank, with its automated retrieval system, broadens the field of consideration for the President in critical decisions of leadership selection.

Professor REICH. That makes me think of something that is almost within my own field. It seems to me to be in direct response to that.

In the field of constitutional law, one of the things that is always

amusing to the student of the Supreme Court is that over and over again Presidents have appointed men as Justices of the Supreme Court who they knew well, had seen for years, had known in government and so forth, and then been utterly surprised at how the man did the job. We have instance after instance.

One of the famous ones is Theodore Roosevelt. He appointed Justice Holmes, who had already been a judge for, I guess, 20 years, and was dumbfounded at the kind of judge that Holmes turned out to be on the Supreme Court.

The point I am making is, what is all this information really worth, because we don't have a science of knowing how a man will do a job. If we appoint a man, we have to take a chance, as the President of the United States does when he appoints a Supreme Court Justice for life. That is a pretty big chance. The fact of the matter is that probably 95 percent of this information is utterly worthless to predict what the man will do and for most purposes I would say 100 percent. If it is a place where you can't afford to take a chance—for instance, the man who is going to pilot the plane that I have to fly on this afternoon—I would like to be sure he knows how to fly. I wouldn't like to take a chance on that. I would like somebody to certify that he is a licensed pilot. There is no second chance there.

But not all jobs in this world are quite like that and not all information is that critical. That is the 5 percent that I was thinking of.

For the most part when you appoint a secretary, an assistant, a judge, or anyone else, even if you know him very well, it is a question in the future and I think that people are trying to be more certain of the future than the future allows by using this information. I don't think a computer or anybody else can tell you whether you are hiring a good man or a bad man.

I think this is an effort for certainty where life teaches us that certainty doesn't exist.

We hire faculty members and we try to find out everything that we can about them but they don't always turn out the way we thought. I just don't think that a computer would help us, or anyone else.

The third kind of law that I had in mind is one that would tell a man what was in his own file and give him an opportunity to rebut.

Now, whether in every instance you would also tell the individual who it was who said what about him—a question that we would again argue out in the case of different kinds of agencies and different kinds of settings. But at a minimum, I think everyone is entitled to know. There are these things which have been said against you. There is this kind of information that ought to be answered. Maybe a simple letter will explain it.

The four parking tickets is a good example of that. It occurred to me right away there is a possibility that somebody else was using his car. He got the tickets, but the officer never knows who parked the car and I might find that someone who borrowed my car had gotten four tickets.

In fact, I have known it to happen that you leave your car at a service station and after they get done greasing it they put it out in the street and it gets a ticket and it is their fault it gets a ticket. We have all had experiences like that. There is a simple explanation. Of course, I don't mean a marine ought to be barred from service be-

cause he has a parking ticket but, at a minimum, he should be able to explain. He should be able to say, "I parked my car because I had to go to a very important meeting. I couldn't leave before the meeting was over and the meter ran out. So between leaving the car parked for 10 minutes more and walking out when I was doing something important, I felt I had to stay."

So I am saying that many, many times people can explain things, and only the person himself knows how to explain it. No one else can explain for him.

I think this is a vital protection. The example we had from the chairman was an example of a crime, a crime of overtime parking.

In the case of things that are less than crimes—for instance, being too nervous or something like that—there is all the more reason to explain. You might say I was nervous because my wife was about to have a child that day when this man observed me. I think that is just an elementary requirement.

Again, my principle would be, we should all be entitled to know what information is in the file and have an opportunity to explain it, except in any case where the Congress decides that it is just absolutely necessary to keep it secret. I don't know if there is any such instance, but if there is, it should be an exception and it should be a rare exception.

Those are approximately three laws, just in a general sense, that I think we need in addition to the Constitution.

Mr. GALLAGHER. Then you are suggesting, Professor, that technology perhaps has outrun the law and it is time for us to bring an extensive balance back into the overall picture?

Professor REICH. Well, I agree with that. I talked to an executive of IBM before I came down here and he said a very sensible thing to me. He said, "Don't go down there and blame the machine." He said, "What is the matter is that you don't have good enough laws to protect people. The machine will do the bidding of our society. It will turn out anything you want and there is nothing wrong with computers," and indeed, I hope I haven't come down here and blamed machines. It is a failure in laws.

I said before that I didn't want good intentions, I wanted laws. I say that because, if you take a clerk in a Government office who reviews files, the clerk has to face up to this question of responsibility I mentioned before. Here is a person with something bad about them. "What should I do about it?" he says. "I don't want to get caught by having ignored this thing."

He needs a law to help him ignore something that he should ignore.

Laws stiffen our backbone. If you want the Government employees to hire the man they ought to ignore information which should be ignored, you need a law to make them know that the Government will support them if someone challenges it later. So if the boss comes in later and says, "Why did you take this man on? He has three parking tickets on his record and now he turns out to be no good. See? We should have predicted that."

The answer should be, "I am not permitted to take that information into account. There is a law here which says so." That will keep the subordinate from getting into trouble. As I say, I believe in laws.

Mr. GALLAGHER. Of course, we are running into some trouble right now where we have laws governing certain instruments which people are violating in pursuit of enforcing the law.

The committee is on a parallel course. We are not attempting to turn back progress. Indeed, even if one could, which one can't, that would be a most undesirable attempt. But we are attempting to air the need for updating our laws, and public interest in some of the things that are happening so that these laws can be passed here in the Congress and wherever else it might be useful, in the hope that the Federal Government can set some kind of guidelines.

As Mr. Packard cited earlier, there is a feeling of frustration about all this—that people feel technology is outpacing them, that they are unable to keep up with it, and therefore there is not much that can be done except resign yourself to the fact that you must answer the questionnaire, you must take a lie detector test, you must expose your entire life and stand psychologically naked before anybody who wants to take a view of what your posture is at the moment you apply for a job.

In this way and by this means you really have stimulated our own thinking on this committee here this morning.

Tomorrow we are going to have the Government witnesses who are advocating the central data bank.

Do you view this as a necessity and, if so, would you like to comment specifically on the concept of a Federal data bank for the collection of information to be used for broad-gage planning?

Professor REICH. Well, the simple answer to your question is, I do not view it as a necessity. As a matter of fact, I think it would be largely useless. Not only is it not necessary, but I think one of the things about our present-day society is that we are flooded with information that is useless to us. We have so many thousands and millions more facts than anybody can do anything with that any proposal to have more facts, or have them more readily available is suspect from the beginning. I don't want to know all the things. I can't keep track of all the things that happen in my own narrow field. Nobody else can either, and so I think we suffer from heaps of useless information. I think that often the only thing the information does is harm. I think this is a wonderful illustration of it.

I think as to the data center itself that it would very frequently do harm, that it is difficult for me to imagine when it would actually help somebody to select a good employee. I would say in one case in a thousand it might help, but I am not even sure this is true. It would not help me to pick an assistant to know what he had done wrong in high school or anything of that sort. As for how it fits into our society—one of the things you have to think about is that the Federal Government sets an example. If the Federal Government does this, it is natural for private employers to think this is the right and necessary thing to do. The Federal Government is something that most of our people look up to and if it says we have to do this, it seems to me that every businessman is likely to say the same thing, so I think it is a mistake to set a pattern like this unless you think it is the kind of country we want to have.

As I have already said, I think very emphatically it is not the kind of country we want to have. It seems to me it would create a cate-

gory of marked individuals. I will use one of my colleague's phrases when we talked about this in a faculty meeting one day. He said we would be tying a tin can around this man. All the rest of his life, wherever he went, he would have a tin can jangling along behind him. I think this is a proposal to tie tin cans around all kinds of different people, some of whom are guilty, some of whom are not, indiscriminately. It is like marking people by cutting their ears or something.

Mr. GALLAGHER. The "Scarlet Letter."

Professor REICH. That is right. That is a more American example and it is a very good example. I think it is a very good example of a proposal where it is not necessary.

Mr. GALLAGHER. The present proposition that we are considering is not necessarily a data center to select individuals for employment although there seem to be many areas where this presently exists. The present proposition is one in which the 20 collecting agencies would centralize the information they have collected, distribute it—ostensibly for such purposes as broad planning of cities and urban renewal—and much of the data could be used in the long-range planning of the Federal Government.

This is the foot in the door as we see it to the further use of central data planning. Would you accept it on the narrow base that is presently offered?

Professor REICH. I would not, unless somebody showed me how this would help the planners to plan. I work in the field of planning and I teach a course in it. I am never sure about why they need to know X or Y or Z for a plan. For instance, if you want to decide we need new housing, do we need this kind of information I was talking about today to know that we need new housing? I don't think we do. I don't think it would help us a bit. It is again an example where most of the things that we know don't help us to make decisions and they get in the way.

That is to say, I would like the planners to go out and work on getting better housing and not spend their time reading all this useless information. I would like them to get to work and I think the more they leaf through heaps of paper, the less time they will have for planning.

Unless somebody says, "We want to know how many people live five in a room in New York City," now that would be useful. That isn't information about individuals with names. If I were trying to figure out where we needed housing, I might like to know that, but I wouldn't necessarily like to know about the emotional stability of the five people in the room. I think they would have to be pretty stable to be able to stand each other, but that is all I would need to know.

I should say, sure, some information is needed, but probably not this. I would say the burden of proof is on those who propose it to show that it is valuable.

Mr. GALLAGHER. Some of our economists and our planners feel that one of the great sources, untapped, for information, is in the Bureau of the Census. That is, that it is this kind of information they would like to have access to—even though I understand last week they came up with a planning concept which showed there were 1 million Indian maidens under the age of 19 who now live in Westfield, N.J. I am not quite sure what the spinoff is, and how accurate this particular

thing is, but nevertheless, this is the kind of information that is acquired.

The economists advocating a central data bank believe that to acquire all this information and not use it is in itself a great waste. This is one of the chief justifications for the establishment of a central data bank.

What would your comment be to that proposition?

Professor REICH. Many of the statistics are already published in general. I mean, there is a great big, thick volume so the economists can find out how many people live in a particular place and they can find out general information of that sort.

I am not sure they are making very good use of what they have now in planning. That is the first thing.

Secondly, I think we seldom recognize how much planning involves decisions which can't be based upon statistics and information. A good example is deciding where to build a highway. You probably read in the paper they are always having a fight about whether a highway should be in one location or another. Those questions don't get decided by information. They are questions of whether you are going to put it through the park or whether you are going to destroy these people's homes, or whether you are going to make it accessible to a factory. They are really political choices, or value choices, and I think a great deal of planning is far removed from the science that it is claimed to be and it belongs in the area of government, judgment, politics, statesmanship. So again I mistrust the people who say we have to know all of these facts in order to plan. My experience is to the contrary.

Again I would say if there is something they find out, like how many three-member families, how many four-member families, how many five-member families do we have, we might know how big to make apartments. That would be useful; but more than that, I question.

Mr. GALLAGHER. You are stating then that the price we may have to pay for this information is way out of proportion to the use to which the information can be put?

Professor REICH. I am saying that and I am also saying it may be useless information that will just waste people's time, in a sense.

In New Jersey I recall a great case in which they limited—they said that you had to have a certain number of square feet in your house. It was a zoning order and a planning order. No one may build a house without a thousand square feet. That was made on a lot of research showing the average three-member family needs 1,000 square feet to live in.

I say, of what earthly use was that study? People have lived for thousands of years in less space than that. Others live in larger space. It is a completely relative question or idea. It depends on who the people are, how big the family is.

It seems to me if they want to have houses of a certain size in that particular township in New Jersey, that is a political judgment and I can make it, but I think to make it on studies and research and statistics is a fallacy.

I think the Center would produce more fallacious than good thinking.

Mr. HORTON. I don't want to completely disagree with you on this, but I want to illustrate how this type of information can be valuable

in the very field in which you are involved. A lawyer's role, of course, is to represent his client and to handle his case, whatever it might happen to be and, of course, law is based on precedent. One of the difficulties that a lawyer has is to spend the time to look up all the cases that have applied to the particular given situation. You are familiar with that type of research.

Now, it is comparable, it seems to me, in the field of law as it is in this other. The planner has to have certain facts and information at his fingertips and if he had to go back and analyze all these things and spend a lot of time digging it out, the same as a legal researcher has to dig it out, that takes time away from his specialty, which is planning. And studying to find out where these lawsuits, or these precedents or these cases are is also a matter of taking up a lawyer's time. As a matter of fact, sometimes the competency of a lawyer is based upon his ability to put his finger on a case. There has been a tendency in our courts, anyway, not to regard the absence of a lawyer having that information to the prejudice of his client. There is a possibility that you can push a button on a given subject and get, in the field of law, all the cases that pertain to that particular subject so that you just have it at your fingertips.

Now, this is certainly a good use of computers, and certainly demonstrates the need for having this type of thing. Perhaps if you think of it in the context of that type of a situation for the planner—and I don't want to argue with you or try to—we could spend all afternoon here debating whether or not it is good or bad, but I think it can illustrate how a computer can be of benefit to a lawyer, or to a doctor—because there are many doctors who don't diagnose a case properly. Xerox has its home plant in my district, and I know they have been giving very serious thought to, and are working now in, the field of providing computers and information for medical and for educational purposes.

A doctor can perhaps, by pushing a button, get backup information for diagnosis or treatment or how he should handle a particular given medical situation. So it does have a lot of benefits.

Mr. Macy, who has to make these decisions—and I don't want to defend him here, but Mr. Macy, who has to make the decisions on hiring personnel, is not in the trained position you are, where you are hiring one typist or one secretary. He is hiring and the Federal Government is losing on a daily basis probably tens of thousands of people. So they have to have some means of getting information in a hurry and not having to spend man-hours in digging up this information.

So I think this is one of the points that should be made with regard to the use of the computer.

I have these points that I have tried to emphasize along with the chairman and that is the role of this committee, to try to find out how that benefit can be harnessed and still preserve that individual right that should be protected.

Professor REICH. I agree with what you say completely. I don't mean to sound like planners should go off to a desert island and know nothing, and I don't think what we are interested in is an irrational society. I mean we try to do things sensibly so, of course, there is information that will be valuable.

I think the job of the committee is to set up categories of information that are valuable on the one hand and does not invade anybody's rights in one category and have another set of information that does invade people's rights.

Precedents in law, luckily, are not people, so if you were to have all the cases ever decided on paper or computers or anything else, we would never have a person's privacy invaded if we just used the reports. That is a good example of where it seems to me no harm could come from a lawyer being able to have the cases at his fingertips. There must be many other kinds of data exactly like that. I would be very happy to have a computer do my legal research for me. I would welcome it and I hope it comes very soon.

Mr. HORTON. They are working on it.

Professor REICH. I know they are, but they are not working fast enough.

The thing we want to do is to focus on the areas where the individual is in danger, where he is going to be scared, where he is going to be scared with reason and not just put our heads in the sand in general. I hope that was clear from what I said.

Mr. HORTON. I think your testimony before this committee has been very helpful because you have set out some basic areas in which we should be very concerned. I think you have sort of steered us through some aspects of this problem, especially on the constitutional law question. I think it has been very helpful to the committee.

Mr. GALLAGHER. If you did have an opportunity to submit a short brief to the committee outlining your proposals, we would be very thankful, especially as to the basis for regulating interstate corporations and for the regulation of problems relating to State governments and the county and city governments, the overall proposal—how you would arrive at, for instance, a proposal to limit intrusive questioning and enforce this at the local level.

If you had an opportunity to give that some thought and submit a brief to the committee, we would be very pleased.

Professor REICH. I think I will be able to do that. I will at least try. I will try to say some of these things I have said here in a shorter fashion and more precisely.

Mr. GALLAGHER. You can say them in writing just the way you have said them here. We are very appreciative.

Mr. CORNISH. In regard to your second suggestion for a law, I am concerned about the individual citizen who submits information to the Government for a specific purpose. By way of example, let's take the person who submits information on his income for one purpose—and that is to have his taxes computed for him.

Do you feel there is any element of contract in this thing? In other words, the Government asks you to provide your income data to compute your taxes and therefore they should not use it for any other purpose, or is there in a sense some informal or perhaps even legal contract that exists in a situation like that?

Professor REICH. I would call it a moral contract. I would be glad to use that notion because I think that it is a sort of an understanding by the citizen of what is fairly expected of him.

Mr. CORNISH. You did not use the word "contract" in your discussion of that. I wanted to know whether you did feel there was an element of contract in such an arrangement.

Professor REICH. I would not use it in its legal sense because the Federal Government, which is sovereign—I am just being a technical lawyer for a minute—does not make contracts with its citizens. It may ask them for what it needs and whether they like it or not they give it. That is the nature of the sovereign, to make laws and people have to obey. I would prefer to call it a moral contract of what citizens understand they are being asked for. This information is being asked for a purpose and they agree with the purpose and they agree it is necessary or they would not agree to its use for other things. In that sense I think it is a very good phrase because I think it implies what most of us feel.

It implies the same thing and again this is not a technical use of the word “contract” but if you call me up in 3 days and say, “So-and-so has come in here and is looking for a job. Is he a good man?”

You don’t say so but there is implied in the call, a notion that I am helping you to find a man. I don’t expect you to repeat what I say to everybody down the street. That is not a contract either because we did not exchange money and so forth, but it is an understanding. I would be kind of upset if I then saw that you told the press or somebody else what you have heard from me.

I think while we do not want to use the technical word “contract,” I think that people sense their Government is dealing fairly with them is a very important thing. People ought to believe their Government is treating them fairly and the tax case you gave is a very good illustration of that. I will stick with the word. Glad to use it.

Mr. CORNISH. That is all.

Mr. GALLAGHER. Mr. Romney?

Mr. ROMNEY. No questions.

Mr. GALLAGHER. Mr. Forsyth.

Mr. FORSYTH. Can I make just one observation? I think you said the economists are not making good use of the material the Census has now. This very argument has been advanced by the economists as a full reason behind this data bank. Somewhere we have to get our definitions a little sharper to find how these go together or conflict.

Professor REICH. I would like to know what information they did not have that they now need and why they need it.

Mr. FORSYTH. Do you have Mr. Dunn’s report, by the way?

Professor REICH. No, I do not.

Mr. FORSYTH. You probably ought to get that before you write your brief. It might be valuable.

Professor REICH. I think it is a question you can answer only in the concrete, and planning covers everything in the whole country.

Mr. FORSYTH. It is too broad to discuss.

Professor REICH. Should we have a train that can go from Washington to Boston in 2 hours? That is a planning question. I do not know what we need to know to answer it. I would say “yes,” offhand, but maybe the answer is “no.”

I think we would agree in most instances that it is important to get down to specifics about that.

Mr. FORSYTH. That is all.

Mr. GALLAGHER. Professor, while it is not necessarily germane to this hearing, there seems to be a climate of concern now existing in the

country as to various matters relating to privacy. We appear to be on a drift course to some extent on questions of wiretapping, bugging, invasions of privacy through all sorts of means, credit evaluations. We find overzealous law enforcers breaking the law to enforce the law they are sworn to uphold.

I think that there is quite a fear now existing that the Government may not be treating its citizens fairly or that the citizen is overpowered and must resign himself to the fact that the rules are now different.

While the Magna Carta was not written just for the king's men it appears that the king's men may well be rewriting the Magna Carta, to make it easier to collect taxes, or whatever the problem may be.

Would you care to comment on that?

Professor REICH. I agree with the thought. It seems to me that we should realize these things usually happen because people are trying to do their job, trying to do it too well. I don't hold to the theory that bad people do these things. I think good people do. The policeman tries to do his job and a civil service man tries to do his job. All of us require laws to remind us of all the other things in society that matter besides our own jobs. That is what a law is. It is a statement of something more general than your own personal concern.

In other words, I might see a diamond ring on the table and I would like to have it, but a law reminds me that other people have interests in the diamond ring. Someone else owns it and someone else cares about it.

A law is to give you a sense of something beyond your own task. I think that in a society like ours privacy disappears just because there are so many people. We are all so crowded together that what was taken for granted in the old days now is threatened by the simple fact of modern life. What we did not need laws for before, we do need laws for now.

When a man could have a quarter section of land and a house on it, he probably did not need a law to protect his privacy. He was probably lonely most of the time and would like to have his privacy invaded. As the times change, you begin to need laws where you did not before. I think that the country is going to keep on growing. It is going to get more crowded and what was once taken for granted is now a precious thing to try to save, try to preserve. I do not think that life would be worth living without some space left for the individual and so I think it is the job of a Congress that wants to plan for the future to look ahead to preserve the values that are threatened by changing times.

I see this as a job to keep our laws up to date with the conditions of modern life. I think that is what this subcommittee is doing.

Mr. GALLAGHER. On behalf of the subcommittee, Professor, we want to thank you very much for the splendid contribution and for stimulating our own thinking, and also for the valuable thoughts that you have contributed to this problem and to reassuring us that by updating our laws, in your opinion, that the world will still be a very desirable place to occupy and this country can, once it brings a sense of balance to fast-moving technologies, be a very desirable place to continue life.

I think that one of the main problems—and I certainly agree with you—is that we must update our laws in view of the rapidly changing complexion of our environment. For your contribution to our enlight-

enment to what we hope will form the foundation for the updating of our laws, on behalf of my colleagues I want to thank you very much.

Professor REICH. I thank you very much for the chance to appear here.

Mr. GALLAGHER. The committee will stand adjourned until tomorrow morning at 10 a.m. when we will hear the Government witnesses, Edgar Dunn and others, who are the originators of this concept. At that point we will question them on the proposal of the Central Data Bank.

The committee stands adjourned until 10 a.m.

(Whereupon, at 1:37 p.m., the committee adjourned, to reconvene at 10 a.m., Wednesday, July 27, 1966.)

THE COMPUTER AND INVASION OF PRIVACY

WEDNESDAY, JULY 27, 1966

HOUSE OF REPRESENTATIVES,
SPECIAL SUBCOMMITTEE ON INVASION OF PRIVACY
OF THE COMMITTEE ON GOVERNMENT OPERATIONS,
Washington, D.C.

The subcommittee met, pursuant to recess, at 10 a.m., in room 2247 Rayburn Office Building, Hon. Cornelius E. Gallagher (chairman of the subcommittee) presiding.

Present: Representatives Cornelius E. Gallagher, Benjamin S. Rosenthal, and Frank Horton.

Also present: Norman G. Cornish, chief of special inquiry; Miles Q. Romney, associate general counsel, Committee on Government Operations; and John Forsyth, special minority consultant.

Mr. GALLAGHER. The subcommittee will come to order.

The first witness we will have this morning will be Raymond T. Bowman, Assistant Director for Statistical Standards of the Bureau of the Budget, and the officer with the direct responsibility to make recommendations for the establishment of a Central Data Bank. Mr. Bowman?

Mr. BOWMAN. Might I ask Mr. Paul Krueger, who is also from my office, to come forward with me.

Mr. GALLAGHER. Yes. Will you please proceed, Mr. Bowman?

STATEMENT OF RAYMOND T. BOWMAN, ASSISTANT DIRECTOR FOR STATISTICAL STANDARDS, BUREAU OF THE BUDGET; ACCOMPANIED BY PAUL KRUEGER, ASSISTANT CHIEF, OFFICE OF STATISTICAL STANDARDS, BUREAU OF THE BUDGET

Mr. BOWMAN. Thank you, Mr. Chairman.

Mr. Chairman and members of the committee, I welcome the opportunity to appear before this committee to discuss problems of possible invasion of privacy which might be involved in the establishment of a Federal Statistical Data Center. For some time the Bureau has been investigating the general problem of statistical data storage and accessibility.

Electronic data processing has revolutionized the methods of recording statistical information so that such data can be tabulated and used as may be required for statistical analysis. We want to be sure that we are making effective use of new technological developments because: (1) we want to bring all available statistical information to bear on problems which confront the Nation, and (2) we want to hold down the burden of statistical questionnaires on respondents. While making

the greatest possible use of our statistical resources we must preserve the confidentiality of individual responses to statistical inquiries which we have always recognized as the foundation of our Federal data collecting activities.

A committee of the Social Science Research Council discussed the problems and prospects for improvements in statistical data storage and access with me and with members of my staff on several occasions in 1963, 1964, and 1965. It prepared a report to the Social Science Research Council which highlighted certain of the problems of accessibility of statistical data and made proposals for setting up a National Data Center as a way of dealing with these problems. The Bureau of the Budget's Office of Statistical Standards assisted the committee of the Social Science Research Council in assembling certain materials for their report. A copy of their report has been provided to this committee and has had some circulation among interested persons in Government and the academic community.

In order to examine some of the problems of a Statistical Data Center more closely, the Bureau of the Budget employed Dr. Edgar S. Dunn, Jr., as a consultant, to study the feasibility and advantages of a statistical data center and to prepare a report setting forth his conclusions. Dr. Dunn became conversant with many of the problems of data storage and access in the Federal Government when he served as Deputy Assistant Secretary of Commerce for Economic Affairs. He has also had a longtime interest in these problems as an economist and statistician. He has studied many of the aspects of data storage and accessibility as a member of a committee of the American Statistical Association set up for this purpose. Recently, he has been chairman of that committee. When he was a Budget Bureau consultant arrangements were also made for him to consult with technical staff of the Bureau of Standards. His report has been furnished to this committee and has been available to interested persons both in and outside of Government.

At the present time a task force appointed by the Director of the Bureau of the Budget is considering "measures which should be taken to improve the storage of and access to U.S. Government statistics." The task force members are Carl Kaysen, chairman, Harvard University, Cambridge, Mass.; Charles Holt, University of Wisconsin, Madison, Wis.; Richard Holton, University of California, Berkeley, Calif.; George Kozmetsky, Teledyne Corp., Los Angeles, Calif.; Russell Morrison, Standard Statistics and Standard & Poors, New York, N.Y.; and Richard Ruggles, Yale University, New Haven, Conn. The task force has not as yet submitted a report.

I have stated that the Bureau of the Budget wishes to utilize the technological advances in data processing and handling associated with the computer to make more effective use of available statistics in meeting demands for information required to deal with today's problems. More and more we are coming to realize that the problems with which we must deal are combinations of many factors and can only be diagnosed and solved by information which relates the various factors involved. Such interrelations of information by the development of a statistical data center need not pose a threat to individual privacy if such a center is governed by restrictions which prevent the release, either within Government or to persons outside Government, of information about individuals or business units.

It does not appear that interrelated use of information can be provided for by more detailed publication of data by the individual collecting agency or in other ways when the information identified with individual reporting units is not disclosed. The only other possibility is to collect the associated information de novo for each inquiry with increasing costs and burden on respondents.

The Director of the Bureau of the Budget is specifically responsible for holding this burden to a minimum. Both the President and the Congress repeatedly remind him that they expect him to perform well in this area. Thus, we continually try to find ways of using existing records for statistical purposes. We have made some progress in this effort but believe more can be done. For example, by using the Federal income tax records as a source of statistical information, it has been possible to relieve about 1 million small businessmen of the burden of filling out census forms every 5 years. And this was done without compromising the confidentiality of a single return. So successful has this been that the Census Bureau plans to substitute tax return information for census questionnaires for yet another 1 million small businesses.

While we want to do all that we can to bring all available statistical information to bear on any problem under study and while we are continually concerned with the need to reduce duplication by making the fullest possible use of existing statistical materials, we are also vitally concerned with preserving the confidentiality of information reported to the Government.

Our Federal statistical gathering activities are expedited by the prompt cooperation of respondents. While most statistical information is based upon nonmandatory replies to Government inquiries, even mandatory replies are more prompt and accurate because of the Government's proven practice of not revealing information supplied by individual persons or business units. This is a most precious asset. We could not effectively operate our statistical system without it. A statistical data center, therefore, if organized, must maintain confidentiality as to individual suppliers of data while at the same time improving access to statistical information for statistical purposes.

Under law and regulation, information reported to the Federal Government for statistical purposes is not released in any form whereby data furnished by any particular individual or business establishment can be identified. There is general recognition that this practice of confidentiality is sound public policy. Thus, when the Supreme Court in *St. Regis Paper Co. v. U.S.* so construed the confidentiality provisions of the census law as to make it possible to subpoena a copy of a census return held in the files of a respondent, the administration supported and Congress quickly passed remedial legislation to give to the copy the same confidentiality and immunity from legal process possessed by the original.

Maintenance of this principle would be a major tenet of any statistical data center and is clearly required under present law. The Federal Reports Act of 1942, section 4(a), provides that in the event information obtained in confidence by a Federal agency is released to another agency, all the provisions of law, including penalties, relating to protection of the information from unlawful disclosure by the collecting agency are also applicable to the agency to which the infor-

mation is released. Title 18, United States Code, section 1905 provides for penalties (fine or imprisonment, or both, and removal from office) for Federal employees who disclose confidential statistical data. These legal requirements can be reinforced by providing that all information in the statistical data center—under whatever conditions collected—will not be released by the center in such a way as to disclose information furnished by individual persons or businesses.

A statistical data center, as we conceive of it, is a way to improve storage of and access to information for statistical uses. It would not have an interest in building up dossiers on individuals because statistical interests do not center on individual cases. Use of data in the files of the center for other than statistical purposes would be prohibited.

I think, Mr. Chairman, even a reading of the report we have made available to the committee would indicate that some comments about them have been out of context.

In conclusion, let me note that nothing I have said should be interpreted to mean that the privacy of individuals does not require continuing and careful attention not only with respect to information now in the possession of Government, but also with respect to the collection of new or additional information.

I have made my prepared remarks brief. I hope they covered the main points. If there are questions, I shall try to answer them to the best of my ability.

Mr. GALLAGHER. Thank you very much, Mr. Bowman.

I agree that perhaps some of the remarks have been a bit out of context, but I would hope that you would agree that it would not be beyond the concern of all of those of us who have some share of responsibility to ascertain whether or not there could be a breach of confidentiality of the names of millions of Americans whose dossiers would be in a data center. The issue is not whether or not you could legally release them. The issue, to my mind, is whether or not this data will be stored with names so people would have access to this information in a central data bank.

I am sure no one would breach a law to release such information, but the fact that it is in a centralized institution where human beings will have access to it is the chief concern.

If you would assure this body today that the identification of no individual would be in your statistical bank, I think we would be very happy to say "Go about your business, and you have met your requirements or you have met at least the elements of our concern."

Mr. BOWMAN. May I comment on your statement, Mr. Chairman?

Mr. GALLAGHER. Yes.

Mr. BOWMAN. I would not want to say that within the data center, within the statistical data center that I am talking about, there would be no identification of information with an individual, just as the Census Bureau can now identify information about a particular business firm and about a particular individual. You would not be able to use this information meaningfully unless this kind of identification were maintained, particularly by the agency which collects the information or the agency which wants to assemble it for analytical purposes.

But I can definitely assure you, Mr. Chairman, that in a data center the availability of information to the staff of the center would probably be much less than the availability of the information to the staff

of the Census Bureau or the Bureau of Labor Statistics or the Social Security Administration at the present time, because the data center would have this information in machine-readable form and not on individual schedules which any one of the members of the staff could examine.

Secondly, I would emphasize that so far as the statistical data center is concerned, there is no intention to organize the data in the center with regard to individuals; that data in different files, data on different tapes, might certainly identify individuals enough so this information can be associated together for statistical purposes, but there would be no intention and no need for the data center to organize specific records about specific firms or specific individuals so you accumulated a lot of information about individuals. There would be the need for collating this information for special, particular statistical analysis, and there would definitely be a restriction on the giving to anybody, in Government or outside Government, just as the Census now does. The Department of Justice cannot get information from the Bureau of the Census. If they want a return filed by a particular business firm, they cannot get it. It is not a matter of theory.

Mr. GALLAGHER. We are trying to protect your interest and the reputation of Census and the Department by not allowing information to get mixed up with data collected by other agencies where the law is supposed to protect the individual confidentiality and confidentiality has never been a major factor.

Mr. BOWMAN. The other agencies do not have the same law as the Census Bureau, but they all undertake the same practices and I would say, Why can't the data center be governed by law in the same way as the Census Bureau is?

I would like to make one distinction, Mr. Chairman. I do not want to make my comments now with respect to all kinds of data centers, nor that this is a grand data center for all kinds of purposes. In other words, there is no use in the Federal Bureau of Investigation maintaining a fingerprint file if they are not to be allowed to use it to identify individuals, but there is no need in a statistical data center when it is being used for statistical purposes, to reveal any information about an individual. I think we have protected it in the past among statistical agencies, not only in the Census Bureau, and we can protect it in a statistical data center. Notice that in my remarks I was very careful to center attention on a statistical data center. The reports we have had have not done this as well as they should have, for they have been more technical. I am talking only about a statistical data center.

Mr. GALLAGHER. You have narrowed it down somewhat from Mr. Dunn's report, and you are zeroing in on the statistical data center aspect of this.

Mr. BOWMAN. The Dunn report and the Ruggles report, while they are not as specific as I now am, were addressed to the same idea. They were just not careful enough in their wording. What they were thinking about and at least what we were interested in, in reviewing their proposals, was not a data center for all purposes, but a Federal Statistical Data Center. We recognize that there are needs for other kinds of data centers for other kinds of purposes, but so far as the data center I am talking about and so far as the data center that the Bureau of the

Budget has been interested in in connection with my work, it has been a Federal Statistical Data Center, not a center for other purposes.

Mr. GALLAGHER. Are you sufficiently confident to say categorically that this will never be used for any other purpose when you have the capacity of a computer to do all sorts of things in this day and age?

Mr. BOWMAN. We have the capacity to do all these sorts of things right now in the Census Bureau. We can do 75 or 60 percent of it.

Mr. GALLAGHER. Let's not talk about the Census Bureau. Let's talk about the IRS. Do you think the same pattern of confidentiality exists there?

Mr. BOWMAN. No, but let me—

Mr. GALLAGHER. You are going to mix this data.

Mr. BOWMAN. Let me make this clear. The IRS data release is governed by law. These laws can be changed. I would conceive of the Federal Data Center as having information from the IRS files in it, but the Data Center would not release that information about individuals. If it were released at all, it would be released under the conditions that now prevail with regard to the IRS and only with respect to its data and by IRS. The Data Center would not itself release that information, nor would it associate that information with anything else and release it in associated form. The kind of data center that I am talking about is a Federal Statistical Data Center which would do a great deal to relieve American business of duplicate reporting, would not reveal information about any individual or any individual business, but would make it possible to bring this information together for statistical purposes when released in statistical form. The identity of the individual would not be disclosed.

Mr. GALLAGHER. Then why can you not give us assurance the identity of the individual or the individual corporation will be eliminated before those statistics will be put into the Data Center?

Mr. BOWMAN. Mr. Chairman, for this reason: Suppose we have certain information in the data that are in the Center from the Census Bureau about individual persons. Suppose we have certain information in the Internal Revenue returns. We do not want to ask the business firms to give us information they have already given us, but we must be able to take the information that we have given to us which are not on the Internal Revenue returns and put it together with the information that is on the individual returns and save them the job of giving us additional information, and make statistical analyses which will indicate various characteristics of the economic scene.

But if anybody comes to us and says, "Give us the information about X company that were on census returns plus the information from IRS," the answer is clear. It can be made a matter of law. Penalties can be placed on the people who supervise the Data Center and operate it. Information about an individual cannot be released from the Center. It is just as clear as that. On this I can give all the assurance in the world.

Mr. GALLAGHER. Are you recommending it?

Mr. BOWMAN. Remember, we are only considering a data center now. If a data center is organized, I would definitely recommend that very clear and specific regulation—legislation if this seems to be the desirable method—be inaugurated with regard to a data center, yes. I am just as much interested as this committee is in protecting the

confidentiality of replies to statistical inquiries, just as much interested.

My life work is in the field of statistics. I am absolutely convinced that the success of the American statistical program is the confidentiality it provides respondents. I am convinced this is true whether the reply is mandatory or whether it is voluntary, because it gets us rid of going through all the weeks of sending it to the legal department in the business firm to see whether they are going to answer it or not answer it.

We have an excellent relation with the business community, and we want to protect that.

Mr. GALLAGHER. Where it is on a voluntary basis and where they know it is adequately protected and not going to be exchanged with other information, the American business community has been very willing to give you information on a voluntary basis. Will not this well of voluntary flow now dry up if they know you are going to put it in a central data bank where the IRS and Census keys might get mixed up some afternoon?

Mr. BOWMAN. Mr. Chairman, all I can say is that we have to assure them in the same way we have in the past.

Mr. GALLAGHER. They have not been very greatly assured in some aspects of some of the agencies that may feed information into the central data bank.

Mr. BOWMAN. I put in my testimony the fact that at the present time in order to save business firms the need for unnecessary reporting, the Census Bureau has been given access under regulations of law to IRS returns. Here you have made in a sense the data center within the Census Bureau. You have added to their own information this other body of information. In this case we are going to substitute one for the other, but in some other instances we will merely be using it to supplement some census information. Everyone is assured that when it gets to the Census Bureau it will not have any less confidentiality than it had in IRS. In fact, maybe they are assured it will have more.

I would hope if we organize a data center, people will be convinced that any data that are put in the Data Center that have less confidentiality in the place where it came from, may still have that less confidentiality there but it will have the greater confidentiality of law to the Data Center. The success of a data center for the purpose that I am interested in, for statistical purposes, is in being able to develop a data center in which that confidentiality will really be recognized.

Mr. GALLAGHER. Of course, if confidentiality does exist, you are performing a very useful purpose; but I cannot help but remember a letter I got not too long ago wondering whether or not one of the dropouts from the IRS lock-picking school might now be in charge of the Data Center.

Mr. BOWMAN. Here we are beginning to introduce a lot of things. Here we are saying—

Mr. GALLAGHER. We are talking about things that are protected by law, and you are trying to demonstrate to me that, despite the great temptation that will now exist for people who have access to information gather by agencies other than their own, no one is going to do it.

Mr. BOWMAN. No, I am not. I am indicating how difficult this situ-

ation gets. In other words, someone has information that a certain individual committed an indiscretion in the past. We have all agreed, the testimony here has indicated, that one of the difficulties with an electronic data machine is that it never forgets it and that man may never be able to get a responsible job any place again if that information is known about him.

Now we are taking an example and saying, "but suppose the Census Bureau or suppose the data center has a person like that." In other words, this person could be employed by the Census Bureau now and he might have access to this information. He could be employed by the data center. I cannot deny that. All I can say is that penalties of law for unlawful disclosure of information have been provided, and I can say that so far as the Census Bureau is concerned, I know of no significant or other than significant instances where information has been disclosed.

Mr. GALLAGHER. Let the Chair take judicial notice that the Census Bureau has been inviolate, and now let us talk about some other things. This has not always been the case with other agencies. Now you are making a mix of other agencies that might have access to that information which we are now discussing, if it is in one central location.

Mr. BOWMAN. Have you in mind any statistical agency, information gathered under restrictions of statistical confidentiality, in which there have been breaches?

Mr. GALLAGHER. No. We are talking now beyond statistical information, even though you concentrate in this area. You fail to give me the assurance that the individual's name will be deleted from your statistics, and it would appear to me we have now placed him in a position of jeopardy unless there are adequate safeguards set up in your data bank.

Mr. BOWMAN. I agree. There would be adequate safeguards.

Mr. GALLAGHER. Is this the telecommunications type of computer that we are talking about, where you would have someone at Census communicate by wire, or whatever the mechanism might be, from the Census Bureau to the central bank for information?

Mr. BOWMAN. Mr. Chairman, I think this is an area, also, which needs very careful discussion. Our consideration of the statistical data center to date has really just begun to examine the various conditions. I cannot say anything more now than what are my own personal views. The data center that we are talking about, the statistical data center, would basically be for data that already have been collected.

Mr. GALLAGHER. The 9,000 reels. Is that what you are talking about?

Mr. BOWMAN. This is information, I presume, which indicated some of the things that might be put in the data center. We have not even discussed in detail the things that would be put into the data center. There are some things that would not be.

The point I would like to make is the data center would not take the place of each of the collecting agencies that now exist, maintaining all of the information with regard to current information. Basically, the data center would be a place where one Federal agency could go and say, "We are dealing with a problem which requires us to have information on other bodies of information than those we now have."

Historic, not day-to-day information. This could be put together for them in a single center.

This is now done, but it is done by one agency or it is going to two or three other agencies to get the job done, or it could be that outside the Government there could be a request for a particular kind of analysis which requires data from more than one agency, but basically of a historic character.

I want at this stage to say we have no idea in mind at this moment of all information collected by all agencies moving to the data center by any kind of wire system.

MR. GALLAGHER. Is this not one of the basic fundamental problems of it all as far as confidentiality and safeguards are concerned? Should you not have a concept now prepared as to whether or not this can be done before you move into doing it? One of the problems with the system that IRS has installed where they want quick results is a quick and dirty system where it has been quickly done, where you do have results immediately, but there are no adequate safeguards installed.

MR. BOWMAN. I know that. I believe that we have not finished our investigation yet. We believe that major economies, major reductions in work done by individual respondents can be realized without doing all of those things at this particular time so far as the Federal Statistical Data Center are concerned.

We believe that this can be done without sacrificing any elements of confidentiality which now prevail with regard to statistical data, which is illustrated by—not comprehensive but illustrated by—the Census Bureau activities. That is what we believe.

MR. GALLAGHER. How can you make that assertion when you do not know what kind of a system you are about to install?

MR. BOWMAN. I know what kind of a system. I do not know what its ultimates will be.

MR. GALLAGHER. I ask you if you are going to have a telecommunications type system from a central data bank to the respondent agencies?

MR. BOWMAN. The answer is at the present time "No."

MR. GALLAGHER. How or what use will you make now of your computers in the various agencies relating to the central data bank?

MR. BOWMAN. Suppose, for example, the Census Bureau now has information on the population census for 1960. It has it on machine readable type.

MR. GALLAGHER. Right.

MR. BOWMAN. The census records themselves now have to be kept, sometimes they are kept in Archives. The Archives is in a sense a data center but a data center in which much of the information cannot be used. If we had the kind of a statistical data center that I am talking about, the tapes for the population census would be in the center in machine readable form.

MR. GALLAGHER. How would they get there?

MR. BOWMAN. Transferred from the Bureau of the Census to the center.

MR. GALLAGHER. How? Hand carried, teletype?

MR. BOWMAN. Runner. Just a roll of tape. How many rolls there would be—

Mr. GALLAGHER. When you roll off on your own machine is it going to simultaneously roll it off in the data bank, or is somebody going to roll it over in the data center and carry it over?

Mr. BOWMAN. It could be done that way. What we are talking about—

Mr. GALLAGHER. This is a fundamental problem involved here.

Mr. BOWMAN. For example, the tapes which the Census Bureau now has from IRS are tapes that were made in IRS that are turned over to the Census Bureau.

Mr. GALLAGHER. How?

Mr. BOWMAN. Physically.

Mr. GALLAGHER. Hand carried?

Mr. BOWMAN. Yes, sir.

Mr. GALLAGHER. That is a very inefficient system. Why would you not have them remain there and use the computers that you now have without centrally locating them, if you have to hand-carry them?

Mr. BOWMAN. If we were set up to do this it might be a better way of doing this. All the technological advances will not be achieved in a moment. All I am trying to make clear is that access to the data by the center, different bodies of data, does not require any relaxation of confidentiality. That is my opinion.

Mr. GALLAGHER. You are assuring me of that but that is not what you are telling me in response to questions I am asking you, Mr. Bowman. We cannot tell, when you get down to it, whether or not we are going to have a data index on every American citizen. We cannot speak in generalities. I think we ought to get to specifics. You have a proposal here that you are about to embark on.

Mr. BOWMAN. No.

Mr. GALLAGHER. You have not really thought the problem out.

Mr. BOWMAN. Mr. Chairman, I do not have a proposal here. We are considering an issue and we may have a proposal which we will want to bring before the Congress. I am not presenting a proposal now. I am explaining to you why we have been investigating the advantages and disadvantages of setting up a Federal Statistical Data Center. I am telling you what I consider to be the major advantages.

Mr. GALLAGHER. I would like to hear the disadvantages. This is what you have not responded to in the question.

Mr. BOWMAN. No. The disadvantage, the one you have mentioned—

Mr. GALLAGHER. I am asking you how will you convey the information that you gather on a confidential basis? How will that be conveyed to the central data bank if and when you ever get around to setting up a central data bank?

Mr. BOWMAN. At the moment much of the information might be deposited in the Data Center in the form of reels of magnetic tape.

Mr. GALLAGHER. Is that compatible tape?

Mr. BOWMAN. If it were not compatible it would be one of the jobs of the Data Center to make it compatible.

Mr. GALLAGHER. What would be the cost of that?

Mr. BOWMAN. Until we estimate it in more detail we cannot say.

Mr. GALLAGHER. You gave us a \$2 million estimate. That seems to be an impossible figure.

Mr. BOWMAN. Impossible with respect to what?

Mr. GALLAGHER. In making the tapes now that you have compatible.

Mr. BOWMAN. I did not give you a \$2 million figure.

Mr. GALLAGHER. It is in the proposal. There is a \$2 million figure.

Mr. BOWMAN. Which proposal?

Mr. GALLAGHER. Mr. Dunn's, I believe it is.

Mr. BOWMAN. We have an estimate by the consultant as to what it would be possible to start a data center for along these lines. We have not accepted any of these figures nor have we actually considered all of the problems that would have to be considered. We have not even considered in detail what would be the best bodies of information to have in the Data Center in its early stages. None of these things have been determined as yet.

Mr. GALLAGHER. Why do you not forget about the whole thing until you have thoroughly thought it out and in several years come back and see where we stand?

Mr. BOWMAN. At the present time, I did not think the Data Center as a data center was in review. I thought what was in review before this committee was the ideas associated with the Data Center and the confidentiality of information or the invasion of privacy.

Mr. GALLAGHER. Are not all of these involved in a central data system?

Mr. BOWMAN. I would like to very honestly answer the question which you think I have not honestly answered, or that I have not specifically answered. That is, it is not possible as I see it to have a data center that is meaningful, even a Federal Statistical Data Center, in which the identity of the individuals for which there is information is erased.

It is possible that the fact that the Data Center has access to this information does not mean that it will be revealed internally within the Government with regard to a single individual. That is the point I want to emphasize in my testimony.

Mr. GALLAGHER. That is a very good point. That is one of the things that I have been trying to direct my questions to. What kind of a system are you going to set up in order to do this?

Mr. BOWMAN. I would hope that we will have a system designed, and we will have a proposal of this character that can be discussed as a definite proposal. We do not have it now.

Mr. GALLAGHER. You think such a system is designable?

Mr. BOWMAN. Yes.

Mr. GALLAGHER. With adequate safeguards?

Mr. BOWMAN. Yes, sir.

Mr. GALLAGHER. Secure with hardware security and software security?

Mr. BOWMAN. Yes, sir.

Mr. GALLAGHER. I hope you tell the Defense Department. They do not think so.

Mr. BOWMAN. I think it is so far as Federal statistical data is concerned.

Mr. GALLAGHER. I am talking now about adequate safeguards to protect confidentiality on transmission to protect against bugging, to protect against interception, to protect against the software problems of who is going to program it, who will have the key, who will mind the tapes, all the human factors involved.

I think the Defense Department has a very vital interest in this sort of a system. If you have a system, I would sleep a lot better at night if your people would go over and tell them how to do it.

Mr. BOWMAN. The Defense Department is talking about a problem somewhat different from the one I am talking about.

Mr. GALLAGHER. No problem is more important than the protection of an individual citizen. This is exactly what I am talking about.

Mr. BOWMAN. That is what I am talking about. The system that I am talking about for maintaining that protection, for improving it, I hope does not involve all of the things that are involved in the Defense Department's operation with regard to the communication of information.

I am very sympathetic to what this committee is trying to do. But I am trying to make my point that a Federal Statistical Data Center can be developed, in my opinion, that will protect the confidentiality of individuals.

Mr. GALLAGHER. Mr. Bowman, do you know of any system now that is set up that is fully secure with regard to radiation transmission?

Mr. BOWMAN. Radiation? I do not know a thing about radiation transmission; no.

Mr. GALLAGHER. I am now sitting in this office typing up a report that is confidential and this report, if we are going to use the computer, ends up being transmitted over to my office. I would assume if you would translate this to someone down in Census typing up statistics about a copy of some sort, this would now be transmitted down to your data bank. That would be a radiation-type transmission.

Mr. BOWMAN. This is assuming we are going to use that method.

Mr. GALLAGHER. I want to know what method you are going to use. Are you going to hand-carry? If you are going to hand-carry, it is not a very efficient use of the computer.

Mr. BOWMAN. Here in a situation—

Mr. GALLAGHER. That is what I am talking about.

Mr. BOWMAN. If you are using the most advanced method you may be subject to a threat of release of information that you do not want to release. Then I would say that in the light of the public interest you may have to deny yourself the using of the most efficient method in order that you may protect the individual against the invasion of his privacy and use a less technologically advanced method.

Mr. GALLAGHER. Like what?

Mr. BOWMAN. You just said hand-deliver the tapes.

Mr. GALLAGHER. Now, if that is so, why can you not do that now?

Mr. BOWMAN. We are doing it now.

Mr. GALLAGHER. Is it working well?

Mr. BOWMAN. It is working reasonably well.

Mr. GALLAGHER. How many users do you have?

Mr. BOWMAN. I would have to get information on that now. We are making tapes available in different ways among different agencies. We think that the idea that we are setting forth here will improve that considerably.

Mr. GALLAGHER. Let me ask you this: How many users have you had? How many customers do you have? How many potential customers do you have? How many requests have been granted? How many have been denied? This would create a demand for the central data bank.

Mr. BOWMAN. Some of the individual agencies could give me information and I will be glad to get it for you as to the demands that they have had for certain of their information. In other words, the Census Bureau has developed a sample of its population census in which in this case the identity of the individuals is lost so far as the user of the sample is concerned.

Mr. GALLAGHER. I am not asking about confidentiality. How many customers do you have for this? How many users?

Mr. BOWMAN. I could find out how many tapes were sold. At the present time it is like asking a new business how many customers it is going to have. One of the things we will want to consider is whether it is worthwhile setting up such a center in terms of the service that can be performed.

Mr. GALLAGHER. Should you not have that information already if you are talking about the need for this as a matter of efficiency?

Mr. BOWMAN. Mr. Chairman, at the present time various statistical agencies are now beginning to develop tapes with information from other agencies. We are in the process now of each agency trying to constitute itself a data center. We are trying to find out if there is not a better way of serving the needs of all Federal statistical agencies just as one group by having the information that it seems appropriate to put centrally located or to have access to it from a central place so that the agencies can use it but without sacrificing the confidentiality of individuals. We think it can be done.

Mr. GALLAGHER. Somebody decided you can do that. Just as a matter of economics, I am sure the Budget Bureau would have an interest in it.

Mr. BOWMAN. We certainly do.

Mr. GALLAGHER. How many potential customers do you have now? How many users do you have? Who will use it?

Mr. BOWMAN. I will get you information on people that are doing this now, if you wish me to. I do not have this information—

Mr. GALLAGHER. Would this not be something that in the beginning should have stimulated the desire for the Central Data Bank or is this just Mr. Ruggles' idea that we ought to have it? Is there a need for it?

Mr. BOWMAN. Let us say it is not Mr. Ruggles' idea alone. A committee was appointed because there is a clear-felt need on the part of a variety of people. They do not have now adequate access to information that is available.

Mr. GALLAGHER. Who?

Mr. BOWMAN. Various members in the academic community, various students of the economy, people who use information in order to—

Mr. GALLAGHER. Do they use it now?

Mr. BOWMAN. They now gather under various hindrances. They think this would improve their access to data without—

Mr. GALLAGHER. Do the agencies who now have the information in these tapes have a list of the users? How many requests have been made? How many requests have been denied?

Mr. BOWMAN. Yes. For some of the things in which this has been done we do have that kind of information.

Mr. GALLAGHER. Does Mr. Ruggles or Mr. Dunn or yourself have this information?

Mr. BOWMAN. I would have access to it. I have not really asked for it. How many—

Mr. GALLAGHER. Is there 10? 100? We are going to spend a lot of money.

Mr. BOWMAN. There are thousands.

Mr. GALLAGHER. How many requests have been denied? Have they ever sought information that properly was turned down? How many times?

Mr. BOWMAN. I presume they have. I cannot testify here and now in detail.

Mr. GALLAGHER. If the Budget does not know, who will know? Certainly not Mr. Ruggles or Mr. Dunn.

Mr. BOWMAN. The Budget may not. I do not know personally because I did not prepare myself for that kind of information.

Mr. GALLAGHER. The question is: We are about to depart from a long-established practice.

Mr. BOWMAN. We are not going to depart.

Mr. GALLAGHER. I would like to know whether or not there is a justification for this departure.

Mr. BOWMAN. Mr. Chairman, we are not departing from a long-established practice. We are adhering to a long-established practice. In a very clear sense any one of the large statistical agencies is a data center now.

Mr. GALLAGHER. Why do we not allow it to continue in the efficient fashion it has in the past?

Mr. BOWMAN. Because we think after we have investigated it a little more carefully that there are more efficient ways of doing so. As it is now the Federal statistical system is a decentralized one. There are many people who feel decentralization is a general advantage for the general collection and development of statistics. There are others who feel differently.

Mr. GALLAGHER. Everybody who is a statistic would agree with this?

Mr. BOWMAN. You would make it so decentralized nobody collected individual information on an individual except one agency. Then you would have an agency for every individual.

Mr. GALLAGHER. No; I do not think we should do that. I think what we are doing now is just fine. I am trying to see some justification as to why we should do it another way. Since you have not designed a system you do not know how many users there are, what the purposes will be, how much it will cost, or why we should do it, I think we ought to abandon it for a while and go back and study it.

Mr. ROSENTHAL. Mr. Chairman, if I may interject a note at this moment. You do not understand it because you have not read that well-received book, "Ruggles of Statistical Gap."

Mr. GALLAGHER. There seems to be a gap involved right here as to why we should do this, Mr. Bowman.

Mr. BOWMAN. We have not yet proposed to do it. We are considering the possibility of making such a proposal so far as this hearing is concerned. We were invited here because there is a great concern about, as there should be, various other developments that are taking place in the economy which seem to involve invasions of privacy. I am here to indicate the way in which I think this will affect a proposal on a Federal Statistical Data Center. I have tried just as clearly as I could to state my position.

I do not believe that I can improve that statement. I think the Federal Statistical Data Center would achieve, could be achieved, and not invade privacy.

Mr. GALLAGHER. You have given a great deal of study to the statistical means for this. Should there not be a corresponding study as far as the desirability of it and as far as the safeguarding of these statistics are concerned, before we start?

Mr. BOWMAN. I am glad you asked that question. It seems to me you asked that question because it seems to me I have not made one point clear.

All my comments are about a statistical data center. This center would not serve a lot of other needs for which other people would say there are needs for centers. I am not commenting on those. I cannot comment on those because they are outside my professional competence and outside of the area for which I have responsibilities. There may be many other kinds of centers proposed. There are.

Mr. GALLAGHER. Mr. Bowman, I have tried to confine our questions to your area of responsibility and to your area of competence, for which I have great respect. I have asked you several questions which I do not feel that you really have responded to. Who are the users? Why? What use has been made of the information that you now have? What compels the necessity of centralization? If you are about to centralize, what kind of a system are you suggesting?

This is one of the things that disturbs this committee.

Mr. BOWMAN. Mr. Chairman, let me answer the first one. Who are the users? At the present time the Census Bureau is a user of IRS information. Other agencies are users of IRS information. Each of them has to make their separate arrangements with IRS.

Mr. GALLAGHER. What is wrong with that?

Mr. BOWMAN. There might be considerable economy if the IRS information were available in one place, better organized for the users, to which the different Federal agencies can put it so that this could be done through one agency instead of having to make arrangements in several different ways. In other words, if the Census Bureau gets information from IRS on data tapes and pays for the cost of doing so, then the question is, if another agency wants exactly the same information and goes to IRS do they do it all over again?

Mr. GALLAGHER. I say "Yes." Let us do it all over again because you want to hand-carry an incompatible tape over to another agency.

Mr. BOWMAN. No, once it was done it would be available to all Federal agencies so long as the agency did not ask for information about individual respondents.

Mr. GALLAGHER. That is done.

Mr. BOWMAN. Did I answer that question?

Mr. GALLAGHER. Actually, you have raised the question that I really must get back to. What kind of a system is going to make this fully protective to the individual? Is there one now in existence? Is there one that has been designed to build in adequate safeguards?

Mr. BOWMAN. Yes, the same system would apply to information in the Data Center as now applies to information in the Census Bureau. They have all this information that you are talking about.

Mr. GALLAGHER. Yes, you are telling me that this can be done. Anybody in the computer business that we have spoken to advises me that it cannot be done.

Mr. BOWMAN. You are talking about techniques of communicating information.

Mr. GALLAGHER. We are either talking of hand-carrying tapes or telecommunications. What are you talking about?

Mr. BOWMAN. I am not willing to talk exclusively about either one of those but I am willing to say—

Mr. GALLAGHER. There are not many other areas involved here.

Mr. BOWMAN. If the objection is to telecommunications, I think it could be established that there are considerable advantages to a data center even if you had to hand-carry the tapes. I would not want to rule out—

Mr. GALLAGHER. Is that what you are recommending? Hand-carry tapes to agencies and use computers?

Mr. BOWMAN. Hand-carrying?

Mr. GALLAGHER. Yes. If you are ruling out telecommunications you are now—

Mr. BOWMAN. I have not ruled it out. I have said that it is not exclusively necessary in all areas.

Mr. GALLAGHER. Mr. Bowman, with all due respect, if you are ruling out telecommunications, why can you not now use the hand system we have and hand-carry tape for those people who wish access to it if they are legally entitled to access to it?

Mr. BOWMAN. Mr. Chairman, much data collected by present agencies, and which use computers, are collected in regional offices. We do not have a situation now for communicating the information in the regional offices, telecommunicationswise, in many instances to the agency which is responsible for tabulating the data. We do not have that now.

Mr. GALLAGHER. Are you recommending telecommunication now?

Mr. BOWMAN. Am I recommending it extensively in every area where it is possible?

Mr. GALLAGHER. No, for the general purposes of your central data bank and regional offices and departments that will be participants.

Mr. BOWMAN. To the extent to which I would be willing to recommend it, we have not studied it yet. You see, this hearing is in a sense preliminary to any proposal that we are bringing before the Congress. We have not finished our job yet. We have not completed our review.

Mr. CORNISH. Mr. Bowman, in one of the reports it is suggested that telecommunications might be used to provide the information from the Data Center to the users; is that true?

Mr. BOWMAN. That is right.

Mr. CORNISH. I think that possibly is one of the points that the chairman is trying to make in this regard. That is an idea which is before the Budget Bureau?

Mr. BOWMAN. That is right. I think we will want to investigate it and we will want to look very closely at whether or not this provides the opportunity for disclosing, for invading anybody's privacy. This is one of the things that will have to be examined.

Mr. GALLAGHER. It should be an essential thing that it be examined by somebody before it is set up and the same machine call off the kind of information they should not have access to.

Mr. BOWMAN. Suppose you do not reveal the identity of any individual?

Mr. GALLAGHER. Can you assure me that it would not? You are not assuring me that you will not eliminate individual identification. If you do, we can say it is a fine thing.

Mr. BOWMAN. I am not assuring you that there will be no information in the Data Center that does not reveal the identity of an individual. I have not said that I would recommend any system of telecommunications which is itself subject to revealing the identity of individuals.

Mr. HORTON. Mr. Chairman, on that point.

As a matter of fact, affirmatively, you have to have the identity of the person or the corporation in order for the statistical information to be of any benefit?

Mr. BOWMAN. In most instances; not in all.

Mr. HORTON. Let us not quibble over words. You have to, in order for this proposed Center to be effective, have the identity of the individual or the corporation furnishing this information?

Mr. BOWMAN. That is what I said in my—

Mr. HORTON. No, you did not say that.

Mr. BOWMAN. Just a minute.

Mr. HORTON. I did not understand that. Let us put it that way.

Mr. BOWMAN. I am very willing to say, and I thought I did say—and I think the transcript will show that I did say—that I could not commit myself to Mr. Gallagher's questions. I could not answer it by saying that there will be nothing in the Data Center that does not reveal—there will be nothing—the Data Center will have no information that reveals the identity of an individual.

Mr. HORTON. I do not want to quibble over words. I am saying to you that you have to state it affirmatively in order for the statistical information to be of any benefit. You have to have the identity of the individual or the corporation or the organization in that data bank.

Mr. BOWMAN. I do so state.

Mr. KRUEGER. May I comment on the question that you are raising here with regard to systems of communication. I think we can say most emphatically that unless the technological advances in the general area of telecommunications or between computers is advanced to the point where this kind of system can be used with sufficient safeguards protecting confidentiality, we would not propose its use.

Mr. HORTON. That gets back to the question of how are you going to protect that confidentiality?

Mr. KRUEGER. What we had thought of was the same kind of protection we now have which requires agencies which collect information under pledges of confidentiality to maintain that confidentiality and which have provisions in law imposing penalties for anyone who violates that.

Mr. HORTON. You are talking about a present system that is quite different from the system that you are now proposing or that you are at least considering. At the present time in many of these agencies they have computer banks already. Is this not a fact?

Mr. BOWMAN. I think we are not proposing a system that is significantly different from the system we now have. We are proposing—

Mr. HORTON. You may not feel it is that way but it seems to me that it is.

Answer this question: Are there not now in existence in various agencies throughout the Federal Government these computer banks?

Mr. BOWMAN. Yes, sir.

Mr. HORTON. What you are proposing is an octopus. You are going to put the head on all these figures because each one of these agencies has these data banks already. So what you are going to do is provide the body for these arms and you are going to put all this information in one central place and then any other department will be able to get that information, will be able to get it on a moment's notice, and conceivably the thing we are concerned about is that this type of information can become public knowledge.

Mr. BOWMAN. That is a very good way of stating it. I think to a considerable extent it represents the background of our thinking about this matter. Suppose it is true that all of these agencies that now collect statistical data, they do not all have banks of data of other agencies now but a great many of them do. Suppose they all had it. What is protecting the confidentiality of that information now?

Mr. HORTON. That is what I am concerned about.

Mr. BOWMAN. I think it would be much better. I believe it is still protected but I think it would be much better to have that information assembled in one place under strict rules of confidentiality that can be much more clearly watched than having it spread over several different agencies all of which are trying to practice rules of confidentiality but they may not all be everything that we would hope they would be.

Mr. HORTON. I understand there is a proposal—I don't know what the status of it is, but that the National Crime Center, which is on a computer basis, is being considered. They will be able to get quite a bit of information. This information, whether you hand carry it, or send it by telecommunications, will end up in this central data bank.

I notice Mr. Macy—and you are probably familiar with his article in the Saturday Review—said “for proper decisions in these areas,” meaning decisions on personnel planning, jobs, and so forth—

In forecasting manpower needs and important decisions of career planning, for proper decisions in these areas, we must have integrated information systems. This will require the use of information across departmental boundaries. It is here that current efforts to standardize symbols and codes will pay dividends. Direct tape-to-tape feeding of data from one department to another may become common.

Now, that is Mr. Macy talking. He is going to be one of the users of this information. If the President or any other agency has a demand for a certain type of personnel, they are going to make a request on your central data bank.

Mr. BOWMAN. Not our data bank, no.

It says information systems. I think this is where I agree with all the things I have heard here today. The thing we are talking about is not making or not even discussing a proposal for a single, all-purpose data bank. What I am discussing is a single-purpose data bank of not all information that is available but of information that is particularly relevant for statistical purposes which is basically quantitative information. It is measurements of one sort or another. But, irrespective of the fact that it might have some information in the statistical data center that is in another data center for other pur-

poses, so far as the statistical data center is concerned it would not release any information about the individual.

Mr. HORTON. It might not, but the other agency might.

Are you telling us now you would not make the information in your centralized data bank available to the Civil Service Commission?

Mr. BOWMAN. I am certainly doing so on an individual—I am—

Mr. HORTON. Are you saying you wouldn't make it available to the FBI?

Mr. BOWMAN. I certainly am.

Mr. HORTON. Under no circumstances would you make it available?

Mr. BOWMAN. Just as the Census Bureau would not make it available to Mr. Macy, or would not make it available to the FBI.

Mr. HORTON. But you have indicated that this information will be made available to you from the various agencies. You indicated that the Census Bureau information would be fed into this computer that you are proposing.

Mr. BOWMAN. But I am proposing that the Federal statistical data center have the same rules of confidentiality as now applies to the Census Bureau and any information in the data center will not be released by the data center in terms that allow the information to be associated with any individual.

Now, if the data center had some information in it from an agency that didn't have those restrictions, it would still be my understanding that the data center would not release that information. The agency might release it, but not the data center.

Mr. HORTON. I hate to hedge on words, but now I think we have to, and I don't like to do that, but you said the center would not release information that would furnish identification. Now, that would mean to me that you would release information.

Mr. BOWMAN. If the center had information about an individual, no matter how it got it, it was in the center, and Mr. Macy wanted that information about an individual, the center would not release it.

Mr. GALLAGHER. Who is going to control the center?

Mr. BOWMAN. Who controls the Census Bureau now? Law. The center would be controlled in the same way.

Mr. GALLAGHER. By which agency, the Census Bureau?

Mr. BOWMAN. We haven't decided where the center might be located.

Mr. GALLAGHER. Some people might pay more attention to the law than others in the Government. For instance, you give great weight to a subpoena. There are other agencies who hand out subpoenas like Kleenex, without much authority—we have had a devaluation of the subpoena process.

Now, you give great weight to it, but other agencies do not. I would be interested to know who is going to run the center.

Mr. BOWMAN. We haven't made up our minds. It might be the Census Bureau itself. It might be in the Department of Commerce closely associated with the Census Bureau. It might be in another agency.

These are the things that are now under review.

One of the considerations in deciding where it would be would be this problem of the history of maintaining confidentiality.

We, definitely, Mr. Chairman, are just as strongly in support of the idea as you are, that for the statistical program which I am mainly concerned about, we do not want in any way to violate the confidentiality of information with regard to the individual.

Mr. GALLAGHER. Assuming we are going to strictly adhere to the law, the problem of computers at this stage of the game is something that bothers us. Electronic radiation transmission problems are still in research and they are only in a research stage at this point. This is one of the reasons why at this particular moment of our time we object and would like to be convinced that confidentiality can be protected. Unless we are all going to start living in lead-lined rooms in this country, and all of the offices involved in the data bank will be lined with lead, there is the problem of anyone getting on the same transmission channel and requesting that information and acquiring that information.

Now, this just has not been solved. I don't know what your feelings are. Perhaps you think it has been solved.

Mr. BOWMAN. No, I don't think it has been solved, but I must admit I don't see its specific relevance to the main idea that we are talking about here.

Mr. GALLAGHER. Its specific relevance is very simple. If I were fortunate enough to have the computer give me a little patronage and give my uncle a job over at the data center, he might see a key lying around and therefore he could turn on the proper channel and recall information on somebody he might not particularly like, or he might have a cousin on whom he would like to do a little double-think kind of operation, and he might flash through one of the erasure-type devices and for all history that person would no longer exist.

Mr. BOWMAN. This can be done now at many of the operations.

Mr. GALLAGHER. Yes, it can. He might exist in census and might not exist in IRS, but he is going to totally not exist in a central data bank.

Mr. BOWMAN. I don't really think so, Mr. Chairman.

Mr. GALLAGHER. Well, not this week, but you know that in the interests of efficiency and economy we will have people in here 3 years from now saying we ought to put a little more information in there.

Mr. BOWMAN. You certainly realize how carefully I have tried to be—

Mr. GALLAGHER. Yes. You haven't gotten around to answering the questions I asked about an hour ago.

Mr. BOWMAN. I think that is unfair, Mr. Chairman. I think that is quite unfair.

Mr. GALLAGHER. No. No. Mr. Bowman, you have not answered my questions as to whether or not there is a system that can protect confidentiality and build in the very things upon which you have told me, and upon which I believe you, and on which we share a concurrence of opinion.

Mr. BOWMAN. If you are talking about an electronic data communications system, I don't know nearly enough to answer that question. There may not be any ways of protecting communication by that method that is completely foolproof against other people tapping in on the system. I would agree with you that the Defense Department knows a lot more about that than I do. But I would say that applies to everything that we are doing now without any changes.

I would say that so far as there being in a statistical data center the information which we now have, in the same general forms as we now have it in separate centers, I see no reason why that information in that center cannot be protected in the same way as it is being protected in the 20 or 25 centers in which we now have it.

Mr. GALLAGHER. You don't see a shade of difference in having that information protected by the law, but subject to a tampering with the law in 25 sections and putting all of this into one area where the same weaknesses could exist?

Mr. BOWMAN. If I see a difference, I see an answer in the centralization.

Mr. GALLAGHER. You don't see the disadvantages to the individual's problem, or the confidentiality aspects? You see no difference in having a centrally located center of information and having it presently exist in 20 or 25 different areas?

The risk has been reduced to acquire information.

Mr. BOWMAN. I don't believe putting it in various pools has significantly reduced the risk, no.

Mr. GALLAGHER. If there is a breakdown in the security of one agency, there is not necessarily a breakdown in the other agencies, but if there is a breakdown in the central data bank, it seems to me we now have a problem.

Mr. BOWMAN. There is, of course, the problem of whether you have all your eggs in one basket or in different baskets, but I would say a well regulated data—

Mr. GALLAGHER. Right there, the egg in the basket. Supposing someone picks up the one basket with all the eggs?

Mr. BOWMAN. You get them all broken. On the other hand, suppose you are very careful about handling the big basket with all the eggs in it and very careless about handling the—

Mr. GALLAGHER. You have not assured me that we have an egg carrier or an egg transmission system fully capable of doing this.

Mr. BOWMAN. Not a transmission system, but I hope I have assured you, Mr. Chairman, that if you can develop a practice of confidentiality as we have in the statistical program, if you can develop that practice and the whole business community and everybody else has confidence in it, that we could develop an agency—maybe part of one of these agencies—that would have all of the data of the various statistical agencies for general use, for which this same reputation would be present.

I hope I have assured you of that. Maybe I haven't.

Mr. GALLAGHER. You have assured me, Mr. Bowman, of your very good intentions. I am not assured that those good intentions can be carried out. That is what worries us. That is what worried us at the very beginning.

May I ask you just one question? Do you now have an inventory of statistical information that is centrally available?

Mr. BOWMAN. An inventory of all statistical information?

Mr. GALLAGHER. That all of the agencies now have.

Mr. BOWMAN. No.

Mr. GALLAGHER. Wouldn't it be cheaper or more efficient if you had an inventory of what data is available in the various agencies now and after a period of a year or two, add up how many requests have

been made for the telephone, how many requests have been denied, and what the problems are, before we get down into a whole new area? It would seem to me that would be more efficient, far more cheaper and protective of the individual. If we haven't done this now, why should we now move into a central data bank when the need has not yet been created or determined?

Mr. BOWMAN. At the back of the Ruggles report there is a practical inventory we made intimating some of the things which seem to be in a form now which would be readily available without us making a decision that we would want to put all of them in the data center, but which seem to be readily available for this purpose. This gives you some idea of some of the things that could be put into a data center. We—

Mr. GALLAGHER. I have read that, Mr. Bowman. What I am asking is, has there ever been an inventory published of the kind of data that is now available—even though it is not centralized.

Mr. BOWMAN. That is the closest thing that I know of to that sort of thing.

Mr. GALLAGHER. Would it not be more advisable to have a full inventory and then distribute it to the potential users to see how many people or what kind of users might want it and how reasonable their requests are before we got into what appears to be the start of a whole new area in government, and not a very efficient operation?

Mr. BOWMAN. We communicate with our public now to a great extent through publications. The inadequacies of publications for many purposes are the things that Mr. Ruggles and the other people of that sort have been talking about.

It would be our hope if we had a statistical data center that operated so that confidentiality could be maintained in the way you say my intentions are, that some of the detailed publications that we now make could be avoided. We might make some economies along those lines. We can never serve the real needs by these detailed publications.

You see, we are all caught in a new system of technology here. We are trying to think our way through it.

Mr. GALLAGHER. We are trying to make sure the people are not caught in the new system. That is why we are here today.

Mr. BOWMAN. Certainly on that basis I am 100 percent in favor of the work of this committee.

Mr. GALLAGHER. Would you consider gathering information and publishing an inventory, before we got into the central data bank, to see what the demands are for this kind of information?

Mr. KRUEGER. It would be the interest in this kind of thing which led the so-called Ruggles Committee to study the whole problem and led them to make a report to the Social Science Research Council in the first instance. These were essentially groups of people—there were people also in the Government concerned with the fact that there is available now a great deal of information; it is stored around in different places; in order to make the kind of uses for statistical analysis, they would like to—they find it difficult to get access to it under present administrative arrangements.

Mr. GALLAGHER. That is not all bad.

Mr. KRUEGER. Not all bad, no, but part of it is and it is the bad part with which we are concerned, which we conceived of, as the formation of this kind of capability as providing a service for.

Mr. GALLAGHER. May I rephrase the question?

Is there now a complete inventory as to the kind of statistics that are now available? For instance, in the 9,000 tapes that you mentioned in your report.

Mr. KRUEGER. No, not a complete inventory.

Mr. GALLAGHER. Has there been a request of Mr. Ruggles and his organization and others who might be interested in this type of information, to make such an inventory and make such a publication to see how many people might want access to this information?

Mr. KRUEGER. We made enough of an inventory to come to the conclusion there is a sufficient amount of very useful information in which a sufficient number of people both inside and outside the government would have interest in, to think that we were warranted in pursuing the idea further and that is essentially where we are now.

Mr. GALLAGHER. How many users make a call on this information?

Mr. KRUEGER. I don't know. That in itself would be a very difficult statistic to get.

Mr. GALLAGHER. This is something we ought to computerize. Have there been 100 people who would want this kind of information? A thousand? How many people have been turned down for making an unreasonable request?

Before we start spending millions of dollars, it would seem to me we ought to determine how many potential users there are. It may well be there are just one or two organizations who are interested in this and perhaps the taxpayer shouldn't be asked to assume this particular burden.

Mr. BOWMAN. Our evaluation will try to take this into account before we come to a regular proposal.

Mr. GALLAGHER. Thank you.

Mr. Rosenthal.

Mr. ROSENTHAL. Thank you, Mr. Chairman.

How much money have you spent to date in all studies and surveys leading to the point where we are now?

Mr. BOWMAN. The Ruggles Committee didn't cost us anything.

Mr. KRUEGER. The Dunn report cost a little over \$12,000.

Mr. ROSENTHAL. At the moment that is the full amount that has been expended in this endeavor?

Mr. KRUEGER. Yes.

Mr. ROSENTHAL. At the moment you really don't have any idea how many users you would have or how many agencies would want it? You are going along on the general assumption that such a thing is useful?

Mr. KRUEGER. Yes.

Mr. ROSENTHAL. Mr. Bowman, is that your position?

Mr. BOWMAN. We are going along on the assumption there has been demonstrated a significant demand for this sort of thing both within the Federal agencies and among the general public but we don't have an actual count of the number of users.

Mr. ROSENTHAL. Has anyone directed a specific inquiry to you asking that such a center be set up?

Mr. BOWMAN. Has any particular agency asked for it? Part of the work Mr. Dunn did was to talk with the agencies. I don't know that there was any particular request for setting up a center.

Mr. ROSENTHAL. Is the movement for this from the inside out or the outside in? Is this a part of a small group who thought this would be a good idea and went out and solicited potential customers, or did the agencies themselves find a need for this and suggest it to the centralized headquarters?

Mr. BOWMAN. Let me answer the question. I have been with the Bureau of the Budget now for 10 years. This has been discussed and suggested in innumerable conversations with me by almost every agency in the Federal Government, yes, and by all sorts of persons outside the Federal Government, State and local governments, individual scholars and a great many people, that there is need for better access and better ability to use the data which is now distributed among different agencies.

Mr. ROSENTHAL. Have you found that private industry has been in the forefront of making use of computers in modern technology?

Mr. BOWMAN. Large industry has, yes.

Mr. ROSENTHAL. Is it part of your idea to have the Government keep up with private industry?

Mr. BOWMAN. I would hope the Government would always be as efficient as possible with modern technology, yes.

Mr. ROSENTHAL. In the case of computerized equipment has private industry taken the lead as compared to the Government?

Mr. BOWMAN. I don't believe so.

Mr. ROSENTHAL. You would agree with the proposition that the Government has special responsibilities in terms of constitutional rights and invasion of privacy that private industry might not have?

Mr. BOWMAN. I certainly do.

Mr. ROSENTHAL. And that in your use of technological equipment, there is this unusual and much harsher but appropriate burden of responding to constitutional obligations?

Mr. BOWMAN. And I would agree that in some instances modern technology might have to be not pressed as far as it could go in order to protect the constitutional rights of individuals.

Mr. ROSENTHAL. Subsequent to this meeting and perhaps before that, you had that as a principle, that you might have to give up some of the advantages of modern technology in terms of the constitutional responsibility?

Mr. BOWMAN. That is right.

Mr. ROSENTHAL. I note nowhere in the Dunn report any comment at all that we have to be aware of invasion of privacy, or individual privacy, or constitutional responsibilities. The closest I come to it is on page 10, the disclosure problem. In very few words nothing is mentioned at all in the whole report about this area of special Federal responsibility.

Mr. BOWMAN. The only way I can explain this, Mr. Rosenthal, is that all of us who were working in this area sort of assumed that it didn't really have to be discussed. In other words, the statistical system has been so imbued with the notion that you do not reveal information about the individual—it didn't get mentioned. I am very sorry, and I think Mr. Dunn is probably very sorry, but you can ask him.

Mr. ROSENTHAL. But those in the statistical field in the Federal Government have a special role as compared to those in private industry, in this area of constitutional rights and constitutional obligations.

MR. BOWMAN. Yes. I think we have a special role. It is not, however, unknown in business. In other words, banks have a recognition of the privileged character of your deposits and other information they may have about you. Doctors have it. Lawyers have it.

MR. ROSENTHAL. On the contrary, in terms of credit information, I think banks and commercial institutions exchange information quite freely and I think they consider that is one of their commercial assets.

In your statement, Mr. Bowman, you list the members of the task force. They are all very distinguished men. However, I do not note that any of them have made their special mark historically in areas of constitutional responsibilities or awareness of invasions of privacy.

In other words, they are all the statistical type, would you say that?
MR. BOWMAN. Yes.

MR. ROSENTHAL. In other words, what bothers me is that—I think the same thing applies to all the members of the committee—there is a group within Government who are statistically oriented and are desirous of following the lead of private industry and taking advantage of computerized facilities who are pushing ahead rather vigorously and yet have taken no overt step either to acknowledge to themselves, to the Congress or to the public, that they have a special responsibility in the field of invasion of privacy.

MR. BOWMAN. But I haven't done that, have I?

MR. ROSENTHAL. Until today, what have you done overtly to indicate that you considered this a special responsibility?

MR. BOWMAN. I did illustrate in my testimony the office and the Bureau of the Budget were very active. The *St. Regis* case; we were active through the lower courts and up to the Supreme Court. We were active in the position that the Solicitor General took before the Supreme Court, which was to argue against the right of the Federal Trade Commission to get the copy of the return from the *St. Regis* Co. The Supreme Court decided elsewhere.

We were active also in helping to sponsor the legislation that eventually corrected this.

All I can say is that the activities of the Bureau of the Budget, my office in particular, have been continuously in the direction of maintaining the confidentiality of statistical information, against its being transferred to agencies that would use it largely for purposes of prosecution or actions against individuals. So the Federal Trade Commission knows that if they came to us with the idea of getting census information that we would strongly support the Census Bureau. If they came to us with the idea of getting information from another statistical agency, we strongly support the nontransfer of that information which identified any individual.

Now, if you say in the writing of these various reports in this area, were we lax in not paying more attention to the writeup of this particular problem, if you want me to plead guilty to that I will plead guilty. Yes, we probably should have made some more mention.

MR. ROSENTHAL. I am not worried about the writeup. That is a trivial thing as far as I am concerned. I am worried about a commitment—as to the nature of your commitment. I have a sneaking suspicion your commitment lies in the area of getting real sophisticated automated technology into the Federal Government so that you can keep abreast of what the large corporations are doing.

I would like to see that commitment matched with the special kind of commitment that we in Congress feel we have to the people of preserving constitutional rights.

The difference of opinion between you and the committee, as I see it, is that we are both in favor of advancing the use of technological equipment.

You think this can be done and still preserve the inherent rights that people have under the Constitution. Frankly, from the testimony here this morning and from yesterday's testimony and other things, I have grave doubts and deep reservations that the national data center can be developed without infringing on individuals constitutional rights—unless Congress enacts laws to prevent you from doing the things that we think should be done.

We can't rely on your good judgment or the good judgment of your associates to prevent these things from happening: Before this center is developed, before any money is authorized or appropriated, I think we are going to have to enact laws to make sure that there are no invasions and that the privileges you are permitted to have to make use of this machine are not abused. This is where our difference of opinion is.

You think we can rely on your good judgment. My own feeling is that we are going to have to rely on legislation.

Mr. BOWMAN. I don't really disagree with what you have said and it may well be that the statistical data center, if it is set up, will require and need, and we will propose that it specify, the passage of laws to protect the confidentiality of information that is stored within it. I don't disagree with you on that.

If I disagree at all, it is merely a matter of saying I don't really want to talk about data centers broadly. A statistical data center where the information is to be used for statistical purposes, I think law can be devised which will protect the confidentiality of information so far as the individual is concerned.

I would also like to answer this question. I think I am equally, as strongly convinced as anyone, that the constitutional protection of individuals is just as uppermost in my mind as is the economy of operations of the Government.

On that point, I am a strong supporter of this point.

Now, with regard to other types of data centers, it may well be that the law will have to make up its mind whether it is desirable or undesirable to have information centralized of a certain kind.

For example, we now have a center for the registration of automobile operation registration. The States and the Federal Government operate this center so that one State can find out whether or not a revocation has taken place in one State that the other State doesn't know about.

Now, this is definitely an infringement, if you will, of some kind on the individual.

Mr. ROSENTHAL. That is not quite the same as sending an employment letter to a professor in school and saying, "What do you think about this fellow? What is his temperament and personality?"

If a man's license is revoked, I see no reason not to tell every State about it.

Mr. BOWMAN. That is the way I feel about it, but every now and again I have a feeling that people are including this as well.

For instance, the writing of a letter to a professor and asking him what he thinks about a person, I can't possibly conceive how that would even get in our Federal statistical data center.

Mr. ROSENTHAL. It would get into an employment or personnel file in an agency and I can conceive that that file in some way could be transmitted or the information therein sent to a Federal data center.

Mr. BOWMAN. A Federal center, but I hope not our Federal statistical data center.

Mr. ROSENTHAL. I don't know a thing about the statistical center and I can visualize this kind of information being gathered and kept in such a center.

Mr. BOWMAN. If it did get there, it shouldn't get out as far as the individual is concerned.

Mr. ROSENTHAL. Right.

Mr. BOWMAN. There will have to be legislation which I hope you will submit and if you fail to act in that regard I suppose the members of this committee will have to prepare such legislation prior to and as a condition, in my judgment, a condition to the establishment of such a concern.

Mr. CORNISH. Mr. Bowman, we understand your testimony is based on the rather current proposals that are now before the Bureau of the Budget, but I hope you will understand that our concern extends into the future a number of years where there may be many pressures and demands to make this computer center something more than what it is presently proposed as.

In that context, I hope you will understand the concern of the committee.

Mr. ROSENTHAL. Thank you, Mr. Chairman.

Mr. GALLAGHER. This might well be incidental, yet it points out the problem: This scientific data business that is going on is all well intentioned, where boys and girls write into a data center and give a lot of information as to the size of their moles and all sorts of other things. That was a lot of fun at the beginning, but now people are running off and selling tapes, catering to the kinds of feelings that they might have.

There is a basic weakness in this also. I think one of the advertisements advertised a \$2.50 a year membership, or a \$400 life membership, which is for the real losers. It shows that the computer really does not solve all the problems. It is one of the things that we worry about, that it might create more problems than it started out solving, and create new problems. Now it is suggested that millions of people will be programed and the lists might be sold for other purposes. So what starts out well intentioned actually could end up very seriously an invasion of people's privacy. All of the bugs have not been eliminated.

Let me ask you this: Is this presently funded, now? Could you go ahead now?

Mr. BOWMAN. There would have to be an appropriation.

Mr. GALLAGHER. But you have a contingency fund.

Mr. BOWMAN. The contingency fund is merely an allowance in the budget but the funds that would come out of the contingency fund would still have to be appropriated. Is that right?

Mr. KRUEGER. It is a contingency allowance in the budget. There is no fund in the sense that here is a pot of money somebody can reach into and get anything out of.

Mr. GALLAGHER. Is it funded now? Can you start it now without any further legislation?

Mr. CORNISH. Using the suggested 9,000 tapes.

Mr. GALLAGHER. The 9,000 tapes that Dr. Dunn mentioned—could you now start centralizing them with the existing contingency fund that you have?

Mr. KRUEGER. I would guess probably that any agency which had funds not required for other uses would have a little difficulty explaining how they might use the funds to go off on this kind of an enterprise without some kind of authorization.

Mr. GALLAGHER. I notice there is a contingency fund in the U.S. budget.

Mr. KRUEGER. If you are talking about the contingency allowance in the budget, that is \$500 million.

Mr. GALLAGHER. Would \$400,000 of that \$500 million have some relationship to the Data Center?

Mr. KRUEGER. Not that I know of.

Mr. ROSENTHAL. You are not going to go ahead and do this without congressional approval, are you?

Mr. GALLAGHER. This is what we want to know here today.

Mr. BOWMAN. No.

Mr. ROSENTHAL. The answer is "No"?

Mr. BOWMAN. Yes.

Mr. ROSENTHAL. Thank you.

Mr. GALLAGHER. You will come up with an answer and a request before this thing gets underway?

Mr. BOWMAN. At the present time we are merely considering this. It probably would be possible for an agency to take on some of the functions of the Data Center, but we have no intention of doing this without a proposal that would be officially presented to the Congress.

Mr. GALLAGHER. And we have now your assurance as part of a legislative record which we are trying to establish here, that when and if your studies are concluded, before you will go ahead, you will come to the Congress and request permission, is that correct?

Mr. BOWMAN. That is right. We would propose it probably as a regular budgeted item and if it requires any special legislation the legislation would have to be drawn and it might well require special legislation with regard to confidentiality.

Mr. GALLAGHER. You might want to propose that when the Kaysen committee report is finished, that it be submitted to a distinguished panel of experts on constitutional law, and invasion of privacy, for their comment and suggestion.

This review would help spotlight the problems that perhaps the statistical people might not consider in their proposals.

Would you feel that that might be a helpful way of bringing about this proposal or helpful in your final decision?

Mr. BOWMAN. Certainly I will discuss this with the Director who asked for this report and indicate this is one of the things that you suggested.

Mr. GALLAGHER. We have two candidates named Reich and Packard whom we would like to recommend for sitting in on such a panel.

As I say, this would be helpful. I think what we have to do is to make certain that we are not going to adopt this without having a real hard look at it from every aspect, from the law, from the invasion of privacy, from the interests of the citizen, as opposed to just the statistical needs.

Now, I would hope that you could consider that suggestion.

Mr. BOWMAN. We shall do so.

Mr. GALLAGHER. Mr. Horton.

Mr. HORTON. Mr. Chairman, thank you.

I start off with the premise that I am not mad at computers and that computers can do good things for us and in my opening statement yesterday I tried to indicate a computer can be very helpful if it is utilized in a proper way.

My approach to this is to try to make it possible for the Federal Government to use computers, but at the same time try to recognize the problem of protecting the individual.

Now, I am a bit confused because I understood that your proposal, or at least the thing that was being thought about, was not so limited as your testimony would indicate here today.

You have tended to indicate that the information that you are going to gather is statistical information and that this would just be a furnishing of statistics to other Government agencies and other users.

Is that accurate? Have you limited the proposal here today? It is not going to be a central data bank for the entire Government; is that right?

Mr. BOWMAN. That is right. Covering all functions.

Mr. HORTON. But you are going to have to get a lot of information. Where are you going to get this information?

Mr. BOWMAN. The idea here was quite broad, that all information useful for statistical purposes and to be used only for statistical purposes would go into the data center.

Mr. HORTON. I don't expect you to have now a definition of "information for statistical purposes," but I wish you would submit to this committee a definition of what you understand "information for statistical purposes" to be. I would like to know that in very much detail.

Mr. BOWMAN. Let me say what I have stated the other way around. It definitely does not involve giving any information that can be identified with any individual. It excludes that. I will try to write out a definition of what it includes.

Mr. HORTON. The present concept excludes giving out information that would be identifiable insofar as an individual corporation is concerned?

Mr. BOWMAN. Yes.

Mr. HORTON. But you have indicated earlier that the information you obtain would identify an individual and would identify a corporation or an organization—would identify the source of information, in other words, and would be very specific.

Mr. BOWMAN. That is right.

Mr. HORTON. So it would be retrievable, would it not, on the data bank?

Mr. BOWMAN. Yes.

Mr. HORTON. What you are proposing also is a bank, a computer bank that will gather all information from all the Federal agencies for statistical purposes only. Is that right?

Mr. BOWMAN. It would gather information from Federal agencies that would be used for statistical purposes, yes. It might include data collected by an agency that didn't collect it for statistical purposes originally. The Internal Revenue—

Mr. HORTON. Would you ask Mr. Macy's department, the Civil Service Commission, for information that they might have on their data bank?

Mr. BOWMAN. I wouldn't think that we would, but I am not sure that there might not be some information that he had that could be useful in a statistical data bank.

Mr. HORTON. Knowing how many people applied for a job at some point, wouldn't that be a helpful statistic?

Mr. BOWMAN. That might be.

Mr. HORTON. Or whether they were male or female?

Mr. BOWMAN. Yes.

Mr. HORTON. Whether they were black or white?

Mr. BOWMAN. Yes.

Mr. HORTON. Whether they were divorced or not divorced?

Mr. BOWMAN. The latter I don't know. I think we might have all the information that he has that is in a form that—

Mr. HORTON. We are talking about statistics now, and not individuals. This would be an interesting statistic or a helpful statistic to somebody, wouldn't it?

Mr. BOWMAN. The thing that I would not see as going into a data center is a written descriptive record about—

Mr. HORTON. I am not talking about any written descriptive record of anybody, but I am asking you if you might not have a call on the data bank of the Civil Service Commission with regard to all the information they had about individuals in a certain category?

Mr. BOWMAN. And the answer is that we might. We might want to tap that into the data center and we might also want to have actual tapes of this information that they have physically in the data center.

Mr. HORTON. Now, if you got that tape and put it in your data center, then it would be retrievable, would it not?

Mr. BOWMAN. It would be, but no one would get it from the data center.

Mr. HORTON. I am not talking about now.

Mr. BOWMAN. It would be retrievable.

Mr. HORTON. I understand your real concern about invasion of the right of privacy at this point, but I am now just asking about the information that could be accumulated and you could accumulate this information.

Mr. BOWMAN. That is right.

Mr. HORTON. In all probability you would accumulate that type of information?

Mr. BOWMAN. In all probability we would accumulate that type of information. We probably would not assemble it by individuals.

Mr. HORTON. All right. Now, if the FBI has a computerized system in which they have all the crime information in the country, might you not want to get that information also?

Mr. BOWMAN. If it were the same kind that you ascribed to the Civil Service Commission, yes, but again we would not want the records with regard to individual criminals, which are written records.

Mr. HORTON. Wouldn't you want to know how many burglars were convicted in a given year, how many people committed murder and all this sort of information?

Mr. BOWMAN. Yes.

Mr. HORTON. You would have to get the specific information from the FBI computer, would you not?

Mr. BOWMAN. That is right.

Mr. HORTON. Have you made a survey as to what agencies have these computers at the present time?

Mr. BOWMAN. The Bureau of the Budget does have a survey of all of the different agencies and this information is available. We haven't a complete inventory of all of the materials of a statistical character that are available in all of the different agencies.

Mr. HORTON. But you have the information with regard to which agencies have these computerized systems?

Mr. BOWMAN. Yes.

Mr. HORTON. Do you know which ones have it now?

Mr. BOWMAN. I cannot name them.

Mr. HORTON. You can furnish that for the record.

Mr. BOWMAN. There is a publication of the Bureau of the Budget that furnishes that.

Mr. HORTON. I think it would be helpful to have this in the record, Mr. Chairman, and I ask that we have this information.

Mr. GALLAGHER. Yes. Without objection, it is so ordered.

(The information appears in app. 1, p. 195.)

Mr. HORTON. Have you any concept of the amount of money the Federal Government has invested in these computer banks at the present time?

Mr. KRUEGER. It is in the same report.

Mr. HORTON. Do you know what it is?

Mr. KRUEGER. Offhand, I do not.

Mr. BOWMAN. It involves the statistical agencies.

Mr. HORTON. I could go through different other agencies that might have these particular banks and you would have this information. You got into some discussion with the chairman as to whether they would be hand-carried or sent over by teletype, and all this type of information. You would have to get some of this information from these various agencies. Would you not have to have the law changed in order to get this information from these agencies which would be so important to you?

Mr. BOWMAN. We might have to have it changed for some agencies. It might, however, be just the same as now—agencies can transfer information to Archives where it is stored. We have not really investigated exactly what limitations there would be with regard to the transfer of information from agencies that now have it into the data center.

Mr. HORTON. Is there not a law which says you cannot transmit information from one agency to another except in the form of statistical totals or summaries?

Mr. BOWMAN. It does not say that you cannot transmit it. It says when you do take it, you cannot release it without—

Mr. HORTON. Reading from section 139(b) of title V of the United States Code:

Information obtained by a Federal agency from any person or persons may, pursuant to section 139-139f of this title, be released to any other Federal agency only if (1) the information shall be released in the form of statistical totals or summaries; or (2) the information as supplied by persons to a Federal agency shall not, at the time of collection, have been declared by that agency or by any superior authority to be confidential; or (3) the persons supplying the information shall consent to the release of it to a second agency by the agency to which the information was originally supplied; or (4) the Federal agency to which another Federal agency shall release the information has authority to collect the information itself and such authority is supported by legal provision for criminal penalties against persons failing to supply such information.

So, you would have to have some type of authority to get this.

Mr. BOWMAN. In many instances, that is right.

Mr. HORTON. Have you talked with any of these various collecting agencies with regard to this proposal so you could find out what the problems are with regard to setting up a central data bank?

Mr. BOWMAN. We have talked with them about some of the problems that are associated with it, but we have not in detail gone into what the limitations would be on each agency. It would be more severe on some agencies than it is on others, because of the pledges of confidentiality that they have.

Mr. KRUEGER. I can illustrate how that might work by an example of what goes on. The Census Bureau operates under very strict statutory limitations which provide that information reports submitted to the Census Bureau can be examined only by sworn employees of the Department of Commerce.

Mr. ROSENTHAL. What kind of employees?

Mr. KRUEGER. Sworn employees of the Department of Commerce. The Internal Revenue Service collects, as you know, income tax returns. They are collected under certain other kinds of restrictions as to the use, availability, et cetera. The Census Bureau and the Internal Revenue Service have been cooperating in an undertaking which involves the collation of information obtained from the economic censuses of 1963 with information from tax returns.

Mr. HORTON. So you are saying there already is an exchange of information between these two agencies.

Mr. KRUEGER. Yes.

Mr. BOWMAN. One-way exchange.

Mr. KRUEGER. Internal Revenue, because of the particular restrictions, is able to make the tax return information available to the Census Bureau, but the Census Bureau cannot make the information from the census of manufactures, say, available to Internal Revenue.

Mr. HORTON. This is a loophole we will have to study, because one of the things I am concerned about is that this thing has been growing up helter-skelter, and nobody has been looking at it specifically as we have.

One of the witnesses yesterday pointed out with regard to the use of the social security number how it began as a confidential piece of information and now it is available to everybody, practically. So, there has been a movement away from the original intention.

I want to underscore something I think we ought to remember all the way through these hearings because I think it sums it up better than any of us can; that is what Mr. Packard said yesterday. He said:

My own hunch is that Big Brother, if he ever comes to these United States, may turn out to be not a greedy power seeker but rather a relentless bureaucrat obsessed with efficiency. And he, more than the simple power seeker, could lead us to that ultimate of horrors: a humanity in chains of plastic tape.

It seems to me what you are doing here for the sake of efficiency is to propose a source of information which can very well get out of hand because you will have to have, for your purposes, identification on that machine.

I give you the benefit of good intentions at this point, but you may not be here 5 years from now and you may not be here 10 years from now. All this information is going to be in that central bank. Somebody, for the sake of efficiency, will say, "We ought to have it for some other purpose." I cannot even envision what those purposes may be. We have to be concerned—and I hope you will be concerned particularly now—about how we are to protect that individual from having that information disseminated on an individual basis. I do not think we have sufficient safeguards at the present time.

Mr. BOWMAN. It is certainly one of my concerns.

Mr. HORTON. Do the people in your Bureau take a close look at what is already being done in these computer centers in the other agencies?

Mr. BOWMAN. Within the statistical agencies, we are quite familiar. We are not familiar with the uses of data in the nonstatistical agencies. For instance, we are not familiar with the uses of data in the Defense Department. We are not familiar with the uses of data in the FBI, the fingerprint files. So far as the use of data in the Census Bureau, the Bureau of Labor Statistics, the National Center for Health Statistics, and all of the areas of our particular concern, we are familiar with the practices which they follow in the use of the computers and the effect it has upon confidentiality.

Mr. HORTON. Do you know of any of these agencies that have come to Congress and gotten the specific authority of Congress to proceed with these so-called data banks?

Mr. BOWMAN. There are some recent acts that were passed. They were data banks broader than statistical data banks. I do not believe any statistical agencies have had any particular authorization in this area. There have been appropriations for their setting up computer facilities.

Mr. HORTON. These computer facilities are more than just statistical, because they have personal information in them. I do not understand what Mr. Macy is talking about, and I wish you would explain it to me, because Mr. Macy indicated there are already integrated information systems, and that they use this information across departmental boundaries. He says it is going to be common to use direct tape-to-tape feeding of data from one department to another. He indicates in this article that they have already used this system to give the President some recommendations with regard to filling high-level jobs.

You would have all that information on that tape. He has only limited information. I assume he does not have what the FBI has on theirs.

Mr. Macy is a very close personal friend, and I have the highest regard for him and I know he is concerned about this problem, but will it not be a lot more efficient 5 years from now for whoever is the Chairman of the Civil Service Commission to say, "We are going to need the information from the central data bank and you have it now in the Bureau of the Budget," and make a request of you and somebody is going to have to decide whether they release it, and they will find some way to release it because it will save the taxpayers a lot of money?

That is a hypothetical question, but it could happen, could it not?

Mr. BOWMAN. It could happen. The thing is, I would think much of the information would not be in the type of data center I am talking about. I did answer all your questions by saying the Civil Service Commission has information of a quantitative character about the number of people, their length of service in the Federal Government, their color, their race, their marital status, and it might well be in the data center.

I also said they could not get it back again if they wanted it so far as an individual is concerned, or no one else could, other than the Civil Service Commission.

Now with regard to files that various agencies may have, with regard to the whole history of a person's employment in the Federal Government, I can see how the Federal Government in order to operate has to know about Mr. X when he worked in this agency or that agency or another agency, and that this information can conveniently be collected and made more accessible. I am not saying that this is inappropriate. I am saying, however, it has risks associated with it that the data center which I am discussing does not seem to have, in my opinion.

Mr. HORRAN. I am pointing out the possibilities and I am also thinking in terms of the fact that there are applications by law students, as was demonstrated yesterday, for employment in the Federal Government, and the Federal Government sends out questionnaires to these law professors and they put personal opinions on those reports. That information can very easily be fed into a computer.

I am concerned about the transmittal and the error in transmittal, too, because this can happen. I had a lawsuit one time where a fellow was charged with a hit-and-run accident in New York City, and he had a pretty bad situation facing him because they had his license. The sergeant had made an error and put the wrong license number down. So, this client of mine was having a really serious problem.

That information will be fed in and it would be put on a tape in Mr. Macy's agency or the FBI or the State Department or wherever it might happen to be. Conceivably, in 5 years from now we will not have a Secretary of State, so somebody will come along and want to get the information on all the people who have studied constitutional law and all the other things that he thinks go into making a good Secretary of State. Then he will go to the most efficient way of getting it, the central data bank. You will be furnishing personal information on somebody which can be reviewed and seen, and it will have a marked effect upon that person's life.

Mr. BOWMAN. We could not release it. I think you have made another point which I think is very important. It may be that we will have to consider not only regulations with regard to what comes out of the data center that I have been talking about, but also regulations about what goes into it.

Mr. HORTON. That is the point.

Mr. BOWMAN. I am perfectly amenable to this type of suggestion.

Mr. HORTON. What goes into that data bank will be very important. I do not think your study or your committee or your task force has been doing much in that connection. You will have a hard time limiting it, because you will be seeking this information from agencies that have it. It will be a lot more efficient for you to get this information from the Census Bureau, and there are some personal questions that are asked by the Census Bureau. There will be a request sometime soon to get that information.

The point I am making is that you have to guard against that.

One other point I want to make is this: Recently the Congress enacted a Freedom of Information Act. Have you looked at that in connection with the implications which might be involved?

Mr. BOWMAN. Yes, I have. In fact, I looked at it very carefully in connection with my business associates, and have been reasonably well convinced that it does not interfere with the confidentiality practices so far as the statistical program is concerned. It does have an exemption in it which indicates that where information has been collected when confidentiality is pledged, it is protected against making the information available.

Mr. HORTON. There is another point I want to make. In your statement you made reference to the fact that there is an exchange of information on Federal tax data to the Census Bureau which is relieving about 1 million small businessmen. I serve on the Small Business Committee of the House, and I am very much concerned about the problems of the small businessman.

One of the complaints that they have is the complaint about so much paperwork. I can assure you from my experience and my personal contact with a lot of these small businessmen, they do not know that this information is being shared. I think this is a problem of communication to the individual that this information is being used for one purpose or another purpose.

In other words, when he submits income tax information, he ought to know that this information is going to be made available to the Census Bureau or this information is going to be made available to the central data bank, and that fact ought to be on the form that he fills out. It is not on the form now, so far as I know. He does not know this. So, when he furnishes this information, one of the problems that I think we are concerned about is how does he get a chance to know what is in that bank so he can contest it if he wishes, or so his rights, whatever they might happen to be, can be represented.

I do not think this point has been considered. Perhaps you might give some consideration to this before you come back with a proposal to form an octopus that is going to gather all this information so all you have to do is push a key and find out all you want about a particular individual, even if you have all these safeguards that you have proposed.

Mr. BOWMAN. I think it is true a great many people do not know, and the only thing I can say is that the transfer of information from the Internal Revenue to the Census Bureau is under provisions of law as it exists.

Mr. HORTON. The law says we are all presumed to know what the law is, but the people do not know what the law is. I have one right

now under the Civil Rights Act. The New York State law is a very wide law permitting people to purchase housing. I have just had a very personal experience. I would say 99 out of 100 people do not know what that New York law is.

That is true of the Federal law, too.

I think when you are getting into this field of personal rights, individual rights and liberty, if you will, they should be put on direct notice that this information will be used in a computer and that type of information will be compiled on them. They ought to have that information in the first instance. I hope your committee will take a look at that.

You see, your task force mission, according to your own statement, was to consider measures which should be taken to improve the "storage of" and then you say "and access to U.S. Government statistics." You put "statistics" in there, but you are talking about the "storage of." You want to improve the storage of and you want to improve the access to this information.

You are building quite a monster here, and I think you will have to watch it pretty carefully before you start centralizing all this type of information that you have.

Incidentally, I am concerned about what has already happened in this field—the storage of information in the FBI, in Mr. Macy's agency, in the Census Bureau, and in the Internal Revenue Service. I think it is a good thing this committee is taking a look at this so we can awaken some people to the problems of what they are facing with regard to giving this type of information.

Thank you, Mr. Chairman.

Mr. GALLAGHER. Thank you, Mr. Horton.

I share Mr. Horton's concern. If this information is available, there will be great temptation to acquire it. You can give us all the assurances in the world that not very many people are going to have access to it, but I just wonder, if no one is going to be interested in it, whether we might be building a great and expensive electronic "garbage pail."

Mr. CORNISH. Mr. Bowman, as it now stands, each individual agency which has this material on tape is responsible for the confidentiality of that material. Is that not true?

Mr. BOWMAN. Yes.

Mr. CORNISH. So, if we set up a national data center, we would impose upon them the same confidentiality restraints, that now exist on the separate agencies. Is that correct?

Mr. BOWMAN. I think more severe than exists on some separate agencies whose data would be in the Center.

Mr. CORNISH. My point is, for example, IRS now has the responsibility of guarding the confidentiality of the tax returns. This proposal actually would introduce a second agency into that same responsibility. So, not only would IRS have the responsibility of guarding the original data that are collected, but also the Data Center would have the same responsibility for any of the material which it got from IRS. So there would be two agencies that would have responsibility for guarding confidentiality, whereas now there is only one in each case.

Do you see any problem at all in the fact that we are spreading the control out a little farther?

Mr. BOWMAN. I think that is a very excellent question. The way I tried to write my testimony and the way I have seen it to date is that the restriction in the Center would be the severest restriction. In other words, continuing the illustration you used, IRS can now make information available to States about individuals. The Data Center could not, under the way I have set it up.

That does not mean that the data could not now be made available to States. It could, because IRS would still have the right to make the data available. They would still have the data.

Mr. GALLAGHER. Are there not 18 or 19 different bodies or people who have access to IRS statistics now?

Mr. BOWMAN. Quite a few. I never counted them.

Mr. GALLAGHER. I think it is 18 or 19.

Mr. BOWMAN. The way I have tried to express it is that the statistical Data Center would have the universal rule, if what I have intended were to come about, that it would not release to anybody information that could be identified with an individual, but many agencies would have data in the Data Center which were not subject to that same restriction. They might release the information, but the Data Center would not.

For example, now and again the Census Bureau may have a request from an agency for information about an individual. The individual may write to the agency and say, "It is all right. Release the information."

The practice there is still not to do it but to write back to the individual and, if he has lost a copy of his form, give him a copy of the form and let that information then be sent by the individual businessman himself.

Mr. CORNISH. This is handled by one set of Federal employees. Under the Center, actually we would have two sets of Federal employees involved.

Mr. BOWMAN. There would be two sets of Federal employees in the sense that the Center would have its own employees. Where the Center would be located, we do not know. It is also true that the other statistical agencies have people that are subject to the same requirements.

Mr. CORNISH. My only point was that you do get an increased problem in the control area.

Mr. KRUEGER. I think one of the points Mr. Bowman made earlier is that it is entirely conceivable that with the operation of a Center of this kind, the present practice whereby agencies now secure information from other agencies would be cut down, because they would not feel the necessity for doing that if there were a central capability of performing that kind of service.

Mr. GALLAGHER. Are we not really, getting right down to it, placing an unbearable burden of temptation on the keeper of the keys or the keeper of the safe—when we get down to putting all of this information into a Central Data Bank—that no one is ever going to want or have access to it?

Mr. BOWMAN. I think we have to impose close surveillance on what goes into the Center.

Mr. GALLAGHER. Assuming you do that, really are we not placing an unbearable burden of temptation on whoever is in control of that?

Mr. BOWMAN. I think not. I think if you expand it so it includes everything known; yes. If you do not expand it that way, I have the feeling, Mr. Gallagher, we might even be improving confidentiality.

Mr. GALLAGHER. Except for an elite who will be in possession of the information. It is that elite that the average citizen has a right to fear if you are going to put military statistics, crime statistics, census statistics, IRS statistics in there, and all that is retrievable if you just press the right button.

Mr. BOWMAN. That is why I said we probably have more carefully to scrutinize and specify what we are going to put in. I am not sure all of the things that people can think of as being there need be there for the Center to perform its most important function.

Mr. GALLAGHER. You have had a great deal of experience and I have great regard for your experience and for what you have done in the Government, but you know that once you start this thing as a "foot in the door," next year there will be someone else who will want to make use of your data bank. If it is that good, it will be expanded, and it will be expanded beyond a reasonable point.

Mr. BOWMAN. I think I agree, except on this point: You cannot stop moving forward in order to be sure that nothing bad will ever happen.

Mr. GALLAGHER. We do not want to impede progress. The computer is here to stay, and it can be a great source for good. We would hope that you are not underestimating the computer. I think you are. I think in centralizing this information in one giant computer, you have not realized the potentialities of the computer, because if you feel that you can control this kind of information and that the computer itself can make this decision, you are not being realistic. You are placing tremendous power in the hands of an elite.

I have a higher regard for the computer's capabilities than I think you have. I do not think we ought to abandon computers. We ought to utilize them as a source for good. But they also can be a source or mechanism for totalitarianism. I do not want to overstate the case, but if all this information is there and someone has total access to it, you can see there are a few dangers in it.

Mr. HORTON. Mr. Chairman, on that point I am not only concerned about the wrongdoer who may seek this information, but I am concerned about the attitude that will be created by this great source of information. The Internal Revenue Service information was very confidential at the start, but now it is available to States and, I think it was mentioned, 17 or 18 other agencies. You can justify every one of these uses of the information. There probably will be hundreds of uses of this central information that you can have that will be very good uses. Every one of us would agree right now that this would be a very fine thing. We want to stop criminals. We want to do this and that. This is a good reason for having this information.

But in the middle of that is a little guy who has now become a statistic. This can cause, I think, the loss of the privacy that he has, and this is what we are concerned about here.

Mr. BOWMAN. Mr. Horton, would you not agree on this point, however: If we make it clear that the center that I am talking about does not release information that can be identified with an individual, then it should be obvious, also, that information should not go into the center if the only reason for putting it there would be because people are interested in getting information about individuals.

Mr. HORTON. I wish we had the time to go into that. I think you have some very impractical impossibilities for curtailing the information that goes in, because you are not going to be able to get information that will be helpful if it is curtailed information at the inception. I agree with the idea. I think it is a good one. I also agree with your premise that we are not going to release anything except statistical information, but, as you have it, you can find out what happened to Frank Horton from the time he was born until right today just by pushing that button—everything.

Mr. GALLAGHER. It might never be released.

Mr. BOWMAN. I hope, however, what you say is not true for the data center that I am talking about. I did try to make this point. There are a lot of ways in which statistical data can be organized for collation purposes. If the data center is organized as I am thinking about it and does not release information about individuals, it would not organize the data that way. It would not be possible to press a button and get all the information about Mr. "X".

Mr. GALLAGHER. Mr. Bowman, we are going to try to adjourn here until 2 o'clock. We would like to finish up, if you do not mind. The kind of information that is anticipated to go into this disturbs me; credit survey, credit information, farm population data.

Mr. KRUEGER. If you are looking at this list as being the kind of information which would certainly go in, that is not true.

Mr. GALLAGHER. I have been looking at a list that has been pointed out as the possibility of going into this. Special census, metropolitan, Louisville, one-time survey; the census population of housing, 25-per-cent sample, population tallies.

There is all sorts of information that will be going in here of a very personal nature. Do you disagree with this?

Mr. BOWMAN. No. All those things have not been decided to go in. They would be available.

Mr. GALLAGHER. These are suggested items.

Mr. BOWMAN. No.

Mr. KRUEGER. This is an inventory of what is available in machine readable form.

Mr. GALLAGHER. This is on your 9,000 tapes now?

Mr. KRUEGER. It is more than 9,000.

Mr. GALLAGHER. Maybe it is more than 9,000. I am talking about the 9,000 tapes you are talking about putting into this as the possible material in the central data bank.

Mr. KRUEGER. No decision has been made of what goes into the center.

Mr. GALLAGHER. I would like to have you put that in the record. That would be helpful. This kind of information would seem to place people in peril and people would—I think, the average citizen who gives this kind of information knowing that it is instantaneously retrievable in a central data bank would walk with a certain amount of justified fear.

Mr. BOWMAN. It is available now.

Mr. GALLAGHER. It is decentralized. Once you centralize it you have a complete profile.

Mr. BOWMAN. Much of this is centralized.

Mr. GALLAGHER. If it is, then let us abandon what you are about to do if it is all that handy.

Mr. BOWMAN. Much of it is not.

The next point is even if it is centralized more than it is now, it is not available now and it would not be available when it is centralized so far as the individual is concerned.

Mr. GALLAGHER. You have told me you are not going to program out the individual's name before it goes in there.

Mr. BOWMAN. I have indicated that legislation to permit the disclosure of the information about the individual is certainly acceptable so far as the data center is concerned.

Mr. GALLAGHER. Right. The legislation is acceptable but the information is obtainable by those persons who have access to the central data bank keys.

Mr. BOWMAN. It is obtainable in the same way it is obtainable now.

Mr. GALLAGHER. Now he has to go to 25 areas and he has to say, "May I have this information?" and he can be turned down at every one of them and I am sure he probably is turned down. Again, I say that you are placing an unbearable temptation before whoever is in control of this central data bank not to use it for nonbenevolent purposes.

I would hope, Mr. Bowman, that you could give great consideration to this before you move forward on it.

Mr. BOWMAN. Certainly.

Mr. GALLAGHER. I appreciate your assurance that this will be submitted to the Congress for full consideration before even a pilot program is set up as a central data bank.

Do you have a question before we adjourn?

We are going to recess until 2 o'clock, Mr. Bowman.

Mr. BOWMAN. Would you like me to be back? I had planned to go off this afternoon but if you want me here I will remain.

Mr. GALLAGHER. Not as long as Mr. Ruggles and Mr. Dunn will be here. We want to thank you very much for being here this morning. I leave assured that you are full of good intentions but I leave with an uneasy feeling that they are incapable of accomplishment.

Mr. BOWMAN. More than good intentions, Mr. Chairman.

Mr. GALLAGHER. Thank you very much.

The committee stands adjourned until 2 o'clock.

(Whereupon, at 12:35 p.m., the committee adjourned, to reconvene at 2 p.m. of the same day.)

AFTERNOON SESSION

Mr. GALLAGHER. The committee will come to order.

The Chair would like to call Mr. Richard Ruggles and Mr. Edgar S. Dunn, Jr., to the stand.

Mr. Krueger, would you like to join in?

Mr. Ruggles, of the Yale University Department of Economics was chairman of the Committee on the Preservation and Use of Economic Data of the Social Science Research Council, which last year submitted a report urging the establishment of a data bank.

Mr. Dunn is a research analyst with Resources for the Future, Inc., of Washington, D.C. As a consultant to the Office of Statistical

Standards, Bureau of the Budget, he has written a review of the proposal for a national data center.

I might say that there appears to be a data wall, Mr. Ruggles, on the campus of Yale University. Professor Reich was here yesterday and took a dim view of your proposal. That is what we are here for—so that we can get all the views, to see that we ourselves can learn as much about the problem as possible.

I hope that this dialog in some way will create a climate of concern necessary before we take such a step.

Mr. Ruggles, would you proceed with your statement?

**STATEMENT OF RICHARD RUGGLES, DEPARTMENT OF ECONOMICS,
YALE UNIVERSITY**

Mr. RUGGLES. The Congress is indeed wise to give serious consideration to the question of the individual's right to privacy, and the possible infringement thereof by the Federal Government, and even Congress itself. The danger lies not only in the massive files which are built up in the different Government agencies, but even in fragmentary information which may fall into the hands of someone who may use it to inflict damage or embarrassment to the individual concerned. The individual citizen is quite right to be wary of a government which can use information at its disposal to coerce, badger, or expose him in ways which are not based upon due process of the law. One of the most encouraging developments of recent years has been the increasing recognition that information obtained illegally does not constitute proper evidence, and that certain agencies of the Federal Government itself may have acted illegally in their attempts to procure such information. Thus wiretapping, improper seizure of records, et cetera, are now considered illegal in situations other than those directly concerned with national security. The use of confessions and the prosecution of offenders without adequate legal representation have also been called into serious question. By the same token, it is becoming increasingly evident that we must take steps to protect the information which the Government obtains from individuals and businesses in its normal operation. This, I gather, is the concern of this committee today.

The problem of disclosure of confidential information about individuals and businesses is not new. It has long been recognized that the information which individuals and businesses provide under law to the Bureau of the Census, for example, is confidential. This means that no other Federal agency is permitted to see or use the individual records, and even Congress itself cannot obtain census information on any individual or company. In fact, this confidentiality has been guarded so zealously that Congress and the other agencies of the Federal Government have been enjoined from obtaining from companies duplicate copies of those records which were submitted to the Census Bureau. The disclosure rules are meant to safeguard individuals so that they can feel sure that information which they give to the Census Bureau will never be used against them for such purposes as tax enforcement, antitrust, or congressional investigations. The disclosure rule has not been interpreted, of course, as preventing the use of census information for analyzing policy or providing in-

formation about specific groups, regions of the country, performance of industries, et cetera. In making tabulations of data, however, the Census Bureau carefully omits those classifications which might enable anybody to figure out information about individual firms or persons.

There are, of course, other Federal agencies which must by their very nature use information about individuals and firms for their operations. Thus for example the Internal Revenue Service not only must collect information about people's income and the taxes they pay, but this information can and should be used to prosecute tax fraud or tax evasion. Similarly, the Social Security Administration must process information about each individual over a period of years, recording his job status, family status, et cetera. This information is necessary for the determination of social security payments. Such use of individual information is of course justified, necessary, and legal. On the other hand, it is a real question whether tax returns or social security records should be turned over to other groups who may wish to use them for other purposes if the persons or firms to whom the records refer may individually be affected thereby. The question of the proper or improper use of information by different agencies is indeed a ticklish one, and procedures should be developed by both the executive branch and the legislative branch which will protect confidentiality and insure the privacy of the individual. In a great many instances, agencies may wish to obtain information not for operating purposes, but in order to make policy decisions and to guide future operations. Thus the Office of Education has a real interest in knowing how college enrollments may be expected to develop in the future. Those concerned with questions of poverty wish to know the dimensions and structure of this problem. In a great many of these instances, the agencies in question have contracted with the Census Bureau to provide them with such general information based upon sample surveys. In these instances, a disclosure and confidentiality rule must be developed which will protect the individual and yet yield the general information which is required.

In addition to the primary question of preserving the privacy of the individual, there are additional related questions which deserve careful consideration.

It is unfortunately true that because the United States possesses a highly decentralized statistical system individuals and, in particular, businesses may be required to fill out a large number of forms from different agencies asking for essentially the same kind of information. Business firms often complain that they spend a great deal of time and effort in making out reports to a variety of different government agencies, and that their life would be considerably simplified if the different groups could get together and make a single request for information which they would share. With respect to sample surveys, it is also true that a number of different Government agencies construct special samples to obtain information which they need for policy guidance, and because these samples are done independently little consideration is given to whether related work going on elsewhere in the Government might not be adapted to serve a number of different purposes at the same time. Careful consideration given to problems such as this might well cut down the bother, expense, and exasperation of

those from whom the information is obtained, on the one hand, and simultaneously reduce the cost and increase the efficiency on the part of the agencies collecting the information on the other.

Recently it has become increasingly evident that detailed individual information is much more useful for research purposes and thus for policy guidance than is aggregated and tabulated information. This is well illustrated by the tax model for estimating the impact of different tax changes, which was developed by Joseph Pechman at Brookings. Under arrangement with the Internal Revenue Service, a set of 100,000 tax returns was developed which represented a sample of all the individual tax returns in the country. The IRS took special precautions to eliminate identifying characteristics, so that the specific individuals could not be recognized. In evaluating the effect of a proposed tax change on various kinds of taxpayers and on total tax revenue, it was merely necessary to program the computer so that each of the 100,000 cases involved would be recomputed according to the proposed change in the tax law. By this device it became possible to evaluate the differences among various proposals, and to see how individuals in different situations might be affected. This research method has proved to be so successful that it is now part of the tax research program carried on by the IRS itself.

The same kind of research technique has recently been used at Yale by a student writing a Ph.D. thesis on the future economic status of the aged population. The primary material used for this research was the 1 in 1,000 sample of households prepared by the Census Bureau from the 1960 Demographic Census. Like the sample of tax returns, identifying characteristics which would permit the recognition of individual cases were removed, but data for each of the households in question was presented in considerable detail. Additional samples of data on household finances obtained from the Michigan Survey Research Center were used to construct a hypothetical income statement and balance sheet for each household, and data on such things as private pension coverage, labor turnover rates for various professions, et cetera, were obtained from the Bureau of Labor Statistics. On the basis of such information, a life process model was constructed, whereby each individual household in the 1960 sample was aged a year at a time for 20 years, taking into account mortality rates, possible job changes, projection of wage changes, and so forth. At the end of the 20-year simulation, the results were summarized to find out what the economic status of the aged population might be, in terms of the income distribution and the nature of those individuals who were at the poverty level. It is true that any single projection requires assumptions about the future social security payments, wage changes, pension coverage, et cetera. However, one of the major purposes of the simulation was to see the extent to which different kinds of assumptions mattered in the estimate of what might take place in the future. It is studies such as this that can help provide a basis for future legislation concerning many of our central problems. Although disclosure of individual information is not necessary, the use of detailed individual information is required.

What kind of satisfactory solution can there be to these problems? First, and foremost, it is essential to protect the individual from an invasion of his privacy and the misuse of information which may

damage or embarrass him. Second, it would be useful if we could reduce the tremendous flood of reports which are required from businesses and individuals at the Federal, State and local levels. Some simplification and rationalization here would considerably reduce the burden on the respondents, as well as the cost to the Government. Finally, however, in developing adequate disclosure rules we must be careful not to throw the baby out with the bath. Many kinds of analytical research require access to individual information, but this should not constitute disclosure in any meaningful sense. Techniques must be developed to preserve the usefulness of detailed information but at the same time insure the privacy of the individual.

Mr. GALLAGHER. Thank you, Mr. Ruggles.

Mr. Dunn, would you like to proceed with your statement?

Mr. DUNN. Yes, sir.

Mr. GALLAGHER. Please proceed.

**STATEMENT OF EDGAR S. DUNN, JR., RESEARCH ANALYST,
RESOURCES FOR THE FUTURE, INC.**

Mr. DUNN. Mr. Chairman, I want to thank the committee for giving me the opportunity to discuss this issue with you today.

I think that the concern of this committee is a very legitimate and proper one and one that concerns me as well. I think it is very wholesome that we can discuss this issue together. I do think that there still remains some residual confusions that I should like to try to point up.

Much of what I have to say here is a recapitulation of my previous testimony and points made by my colleagues. However, I think there might be some merit in recasting them in a somewhat different way.

I think that it is important to recognize clearly that there are two basically different types of information systems: (1) there are statistical information systems, and (2) there are information systems that have as their purpose the generation of intelligence.

I might say that I use the term "intelligence" here with some misgivings and for want of a better term. My concern is that the term sometimes carries a certain amount of emotional freight, but I use it here only to make a technical distinction.

The distinction is basic. Intelligence systems generate data about individuals as individuals. They have as their purpose "finding out" about the individual. They are widespread and common and essential in our private and public business. They include such things as the medical records a doctor keeps to trace the changes in the well-being of his patient and the educational records the teacher keeps to trace the progress of the student. They include requirements essential to public administration, such as the licensing authorities' need to know whether a driver has legal vision, or the tax authorities' need for information to administer taxes.

Most of the intelligence information systems with which I have had any direct contact are restricted systems which have a specific administrative purpose and have not as their purpose the organization of intelligence about individuals into an integrated dossier of any kind.

It is conceivable that an intelligence system of this kind could be developed.

A statistical information system produces information that does not relate to the individual. It only identifies characteristics that relate to groups of individuals or populations. It has as its purpose answering such questions as these: What proportion of the residents of Appalachia possess income less than \$3,000? In what way does the mix of economic activities in New York City differ from Chicago? What activities seem to figure prominently in recent rapid growth of the Southeast, Florida, the gulf coast, and the Boston-Washington corridor? What proportion of the registered voters turned out in a recent primary and how were they divided between Republican and Democrat, urban and rural, white and nonwhite?

These are just illustrations but emphasize the range of the questions, which is infinite.

This is sufficient to emphasize that a statistical system is busy generating aggregates, averages, percentages and so forth that describe relationships. No information about the individual is generated.

No information about the individual needs to be available to anyone under any circumstances for the statistical information system to perform its function.

This distinction, it seems to me, divides the issue of personal privacy into two parts. The first part of the issue is reflected in this question: Can a statistical information system be developed and administered in a way that assures that it cannot be used as an intelligence system? I think the answer is an unqualified "Yes." That this can be done and done successfully there is no doubt. It has been done and done successfully for many years for those files that constitute the records of the Bureau of the Census. We don't have to speculate about possibility. We have demonstrated the possibility.

Let's see wherein this protection does exist and the ways in which it can be extended.

The protections are of two broad types: (a) those that stem from the design and technical characteristics of the system, and (b) those established by statutory and other legal restrictions prohibiting the release of individual data.

I think that it should be emphasized that such statutory restrictions do exist, as has been emphasized here previously. The statutory regulations governing the census files are a case in point. They have existed for a long time. They have worked well to prohibit illegal disclosure of individual data to anyone, and this includes the President of the United States. The details of the legal provisions in this area and their history are sufficiently complex that I am not qualified to review them, but Dr. Bowman here and the men on his staff and men on the staff of the Census Bureau can elaborate on this subject.

These legal prohibitions are supplemented by a formidable array of procedures embodied in the design of a statistical system and inherent in modern technology.

These legal provisions constitute the following:

The lay or public image of such a system is one of an automated monster with everybody's records that can be instantaneously retrieved by pressing buttons. There seems to be no awareness that the same technology that projects this frightening image has characteristics that can be and are utilized effectively to protect the sanctity of the individual record. Let me indicate some of the ways.

First, consider the technical form of the record. You see in my hand a piece of computer tape. This is the form of the record. You and I can't read it. Although there may be several advanced computer technicians in this room, they can't read it. To get any information out of this tape requires (1) a machine, (2) a codebook, (3) an appropriate set of instructions, (4) a technician. You see, when we put information into such a system we start with an inherent technical advantage over traditional records when it comes to protecting personal privacy. Information on paper in agency files can be very easily prostituted by any human being who can read and write and can be bought. The number of people who could get a specific piece of information out of a file of this type are very limited and very easy to identify. This facilitates the establishment of security procedures.

Second, I just said an appropriate set of instructions was necessary to get any information off the tape. This prompts me to make two points.

A statistical system will have the data formatted and stored and will have developed a set of instructions—known in the lingo nowadays as computer software—that facilitate the generation of statistical services. It may, in consequence, not be a very efficient system for intelligence purposes because neither the format of the record nor the standard instructions are developed for intelligence use.

However, there is a more important point. In addition to designing instructions that tell the machine what to do, you can give it instructions that can tell it what not to do. You can teach the machine to distinguish appropriate inquiries—statistical questions—from inappropriate inquiries—intelligence questions or individual data. Furthermore, you can go further than that. You can teach the machine to identify “trick” inquiries—either accidental or purposeful. That is, you can teach the machine to say, “This is a statistical inquiry but it is framed in such a way that the population or group you have defined contains only one individual or less than some specified number of individuals.”

Thus you can design a system in ways that prohibit any output other than a legitimate statistical analysis. The machine itself and the design system that operates it can be used to monitor the use procedures in ways that greatly increase the efficiency and assurance of security.

In addition, through system design and the kinds of instructions you give the machine you can teach it ways to disguise records. For example, you can replace all individual identification codes with a special security code that only the machine can use and which it uses only for the purpose of associating records. Under such circumstances, no one engaged in any part of the productive operation of the system would be able to identify any individual record without access to the set of translation codes that could be protected by special provisions of law and intensive security devices. The machine can also generate data useful for statistical purposes that are randomized or modified into “prototype” records that retain certain useful statistical properties while losing all identity as individuals.

We have had experience with all of these devices, legal and technical; they can be further perfected and extended as we attempt to improve the efficiency of the system for legitimate statistical use.

Indeed, one of the strongest arguments for an improved statistical servicing capability such as I have proposed, is the fact that some integration of procedure and regulation is important in making the best use of the technical safeguards that have and can be developed to assure personal privacy.

So much for statistical information systems. The second part of the issue of personal privacy is related to information systems directed to the uses of intelligence. The issue here is basically different. You can't ask, "How can an intelligence system be designed to protect the output of information about the individual?" That is what it is designed to do and it has many legitimate purposes recognized by law and society. We have already identified examples of these.

Whether or not as a matter of practice the rights of individuals to personal privacy have been adequately protected in these systems as they currently exist, I cannot say. My area of professional experience has never involved me with this type of information system. I would just like to make two observations.

(1) As a layman concerned with personal privacy, my impression is that actual and potential violations of personal privacy are more important and more serious in intelligence systems of this type. It is my impression that this is the area where investigation and reform are more drastically needed.

(2) It should be the concern of Congress that a general-purpose, public-servicing statistical information system should be protected from any use as an intelligence system. I think I have demonstrated that this has and can be done.

I have gathered the impression that there might be equal concern that intelligence systems likewise never be used as statistical systems. This is not the danger. There is not a symmetrical relationship. If you have a properly established and safeguarded statistical system, you can often gain by associated—either permanently or temporarily—records generated for administrative purposes with the statistical system.

For example, the Internal Revenue records or the Social Security records produce as byproducts—that is, things that have to do with their public face, age, sex, race, and so forth—certain demographic characteristics of the population that can be used statistically for making good, economical statistical population estimates for the intercensal years when used in conjunction with benchmark data from the census. Again, it may be useful and desirable to make a statistical analysis of the characteristics of the population of public assistance recipients for evaluation of public policy, in order to evaluate some aspect of public policy.

Such uses of traditional administrative records can be accomplished without any violation of personal privacy. The essential point here is that in the association such administrative records would gain all of the protections of a properly organized statistical information system.

Thank you, gentlemen.

Mr. GALLAGHER. Thank you very much, Mr. Dunn.

You have both pointed out the need, though not very well, of the benevolent uses for which the central data bank is to be used. I was interested, Mr. Ruggles, in the programs that you pointed out as being successful and rendering a valuable service.

However, you, in your statement, said that the personal identification was removed. If it worked successfully there, why could not the personal identification be removed when you assemble data in the central data bank?

Mr. RUGGLES. For practical purposes, it is removed, but you must remember there are many ways of identifying people other than by their names. You take the wealthiest person in a small town. You don't need his name if you know he is the wealthiest person.

Various government agencies have been very wise in preventing the disclosure of individual information which might be used to identify the person even though the name is not given. As a matter of fact, in almost all the machine-readable records that are kept, the name of an individual never appears. An identification number is often assigned as has been suggested. The purpose of this is merely to keep the record straight so if you have an error, or you find something queer about a given case, you can locate it again in the record.

Also, suppose you are trying to match records. For example, you may find certain information is available in Social Security records, and certain information is available in Internal Revenue records and you wish to match it and add it to general demographic information in the census records. You need some way of linking these records. You are not interested in the person, but you are interested in bringing the information together.

Mr. GALLAGHER. In this we share no disagreement, on the necessity of bringing the information together. We are in some difficulty as to the necessity of bringing the individual's identification along with it.

If you say on the one hand it is not necessary, why does it become necessary to have it and centralize it?

Mr. RUGGLES. In many cases there is no other link to bring the information together except a person's name, or a company's name. I think the best case in point might be Internal Revenue records, matching the companies in the IRS data with the establishment data of the Census Bureau, it is necessary to know whether this is the same company. If there is no other linkage than the name, the name is a useful piece of identification. In fact, that is what we use names for generally, so I know who you are and you know who I am. It is a reference device, but it is only used as a reference device.

Mr. GALLAGHER. I am glad to know what we use names for, but I am trying to keep your name and my name out of a pool where if you wanted a promotion there wouldn't be a long trail as to why you shouldn't get that promotion if someone made a bad evaluation of you when you were going to school.

Mr. RUGGLES. Oh, I agree with you completely on that.

Mr. GALLAGHER. Then why do you feel names are necessary? Why should the individual then be identified in the central data bank?

Mr. RUGGLES. I guess it is the same reason why in a demographic census they collect people's names. If you took a census without anybody's names, you would be rather lost if you were studying migration and were trying find where a person moved to or something of that sort in the basic records. Were you to assign everybody a number, you wouldn't need a name.

Mr. GALLAGHER. We have done that already. I am talking about interchanging a person's name and a person's number.

What I am speaking of is, is it possible to establish such a central data bank without personal identification?

Mr. RUGGLES. I would think that for the vast majority of records this would be true, yes.

Mr. GALLAGHER. Would you recommend that be done?

Mr. RUGGLES. If each individual were assigned a number instead.

Mr. GALLAGHER. You are still leaving his fingerprints on your record.

Mr. RUGGLES. That is right. You must link records. In order to link records, you need some form of identification.

Mr. GALLAGHER. Then it is impossible to set up a central data bank without eliminating the identification of an individual?

Mr. RUGGLES. Or company or any other unit with which you are dealing.

Mr. GALLAGHER. Therefore, personal identification would have to be a significant factor in establishing your central data bank?

Mr. RUGGLES. I would say in order to process information, this is correct. There has to be some identification of a unit; otherwise you would have no idea whether you had duplicates in your system; you would have no idea as to whether you had coverage of the same group of people or the same establishments from different sources. It would be what was referred to here as an "electronic garbage disposal."

Mr. ROSENTHAL. There is no way to refine the input in this sophisticated machinery to eliminate that in advance?

Mr. RUGGLES. It would be very simple, as suggested here, to have a key that would assign a new identification number to each unit that you were using so that there would be no visible connection between any record you had and any meaningful identification.

Mr. GALLAGHER. But if you had a key, you could match it up?

Mr. RUGGLES. That is right.

Mr. ROSENTHAL. The key could control a group of individuals so we would have no way to break it down as to who the individual involved was.

It doesn't make sense to me at all. In other words, you say there is no way of eliminating the possibility of error being fed twice into the machine without individual information?

Mr. RUGGLES. You see, one of the problems in bringing records together that you are trying to match, is to make sure, that the records do in fact refer to the same unit. Supposing you have one set of records that tells about the employment of the husband. Another set of records tells about the employment of the wife. You have to bring the records of that household together so that you can see what effect certain factors may have upon the participation of the wife in the labor force. This means there has to be some method of identifying a household. This may be an address. In many cases it wouldn't be a name. The address is used in the case of establishments very often because many times a name is ambiguous. A name is only one piece of information about a unit.

Mr. GALLAGHER. The name is not ambiguous to the bearer of the name.

Mr. RUGGLES. Often it is spelled differently. Sometimes the first name is used instead of the last name or the middle name.

Mr. GALLAGHER. To me it is not an ambiguous situation for you to have all of my records. I know you have my records.

Mr. RUGGLES. That is right, but you would not know that your name was on them.

Mr. GALLAGHER. I would know there was a central data bank and 25 or 30 people would have a complete profile and they would have to go to a lot of trouble to assemble it, but they would not have to go to a lot of trouble for you to gather information you should not have.

Mr. RUGGLES. I believe though the things you would object to would not be that someone would know your name and address and things of this sort. What you would object to would be as you pointed out so aptly before, what someone said about you or what somebody reported, or a previous job or a previous offense, and I would presume that that sort of information would not be germane to these studies, and certainly not germane to a centralization of them.

Mr. GALLAGHER. Let's just stay on what Mr. Dunn has divided it into. We are not talking of the intelligence gathering center, but we are talking about a central data bank. A statistics gathering bank.

It is impossible to set this up efficiently or meaningfully without some personal identification of the people involved; is that correct? Whether by name or number or fingerprints?

Mr. RUGGLES. This would be true not only for this data center, but for Internal Revenue, for Social Security, for Archives, for Census, for all holders of records. Records have to be about specific reporting units; that is correct.

Mr. GALLAGHER. Therefore, these records that would be included in the central data bank would have a trail back to an individual; is that correct?

Mr. RUGGLES. Yes. I personally have never had the idea of a central data bank. That sounds too much like a data morgue and it may well be.

Mr. GALLAGHER. It sounds like a morgue to a lot of people.

Mr. RUGGLES. The Social Science Research Council referred to a national data center which was a clearinghouse or cooperative enterprise with very strict disclosure rules, intended to be a service organization to produce statistical studies.

Mr. GALLAGHER. That definition could fit a bank, except for the last part of the sentence. While we call it a bank, some people might call it a data center.

Mr. RUGGLES. Yes, it is a data center. This is what was recommended by the Social Science Research Council.

Mr. GALLAGHER. Will you please tell me about the Social Science Research Council?

Mr. RUGGLES. It is a nonprofit research foundation that gives grants of money to scholars working in universities on various subjects. It has received money from the Rockefeller Foundation, the Ford Foundation, and it is essentially a grant-making organization—many of fellowships, scholarships, and so on; the grants are in universities. It is concerned with the orderly development of the social science disciplines themselves.

The group that was worried about this problem of information for the social scientist was worried about it in the same way that the scientists are worried about the development of their laboratories and laboratory equipment, and the people in the humanities are worried about the development of libraries.

The social scientists are, to an increasing extent since the computer has come in, concerned with obtaining the kind of information that will allow them to do economic analysis and other social research that will throw light on problems such as legislation, the development of our society in general.

Mr. GALLAGHER. Then you would be a user of the data center?

Mr. RUGGLES. Well, shall we say the profession would be a user.

Mr. GALLAGHER. Well, your organization.

Mr. RUGGLES. It is not my organization.

Mr. GALLAGHER. The organization to which you belong.

Mr. RUGGLES. The organization which requested that I chair a committee on this topic for them.

Mr. ROSENTHAL. How could they be a user of this?

Mr. RUGGLES. They would not be a user of it. They are essentially a professional organization.

Mr. ROSENTHAL. They are interested in fostering the interests of the profession.

Mr. RUGGLES. That is correct. Like any of the other learned societies.

Mr. ROSENTHAL. Did any Federal money go into this foundation which is then dispersed as grants?

Mr. RUGGLES. Not that I know of. They may have gotten some National Science money, though I do not know. I do not know about their finances.

In consulting with the various Government agencies, we found none of them were set up in a way to service either other Government agencies or people on the outside with an analysis of the kinds of information that they had within the agency. Thus, for example, Internal Revenue Service is set up to collect taxes and to deal operationally with the things related to the income tax. They are not organized so as to use as a byproduct the information that comes from the tax forms, for other purposes.

Mr. GALLAGHER. There are some who would disagree with you.

Mr. RUGGLES. Well, this is not their primary mission. They have set up a statistical group to publish the Statistics of Income, but only to a very limited extent do they do contract work from outside for either other Government agencies or people outside of the Government.

The Bureau of the Census has probably done the most work for other agencies and for people outside, but even here the number of requests they must turn down because their primary mission in collecting the demographic census and the other censuses is so large they are incapable of handling every request.

Mr. GALLAGHER. How many requests have been made by grantees of the organization to which you—

Mr. RUGGLES. I don't know. The Social Science Research Council?

Mr. GALLAGHER. Yes.

Mr. RUGGLES. The Social Science Research Council does not undertake studies of its own.

Mr. GALLAGHER. I said the grantees.

Mr. RUGGLES. I have no idea how many grantees there have been.

Mr. GALLAGHER. You have no idea of how many requests have been made for this information?

Mr. RUGGLES. No. I have no idea how many grantees there are. They give out a considerable number of fellowships a year. I just don't know.

Mr. GALLAGHER. Wouldn't that be a significant factor in asking for taxpayers' money? To create this center for the use of people to do studies? I would think it would be germane to determine how many people might want to use this.

Mr. RUGGLES. You can take three approaches to this. You could have a public opinion poll on it and ask people if they thought this was a good idea.

Mr. GALLAGHER. I would think that would be rejected.

Mr. RUGGLES. You could also go for some sort of referendum and essentially get the people's view on this.

Mr. GALLAGHER. I would like to run on that platform.

Mr. RUGGLES. I think I know how both these would come out. But this is not quite the point. If you are running a company and you decide that you need certain kinds of information in order to make intelligent decisions on costs and prices, you don't ask yourself, "After I get this information, how many people are going to use it?" You ask instead, "What is the usefulness of this sort of information to carry out the things that we want to carry out?"

Mr. GALLAGHER. You don't see a difference between running a company and running the Government? A person with a company can quit.

Mr. RUGGLES. Had the IRS in the case of Joe Pechman's tax model asked in advance, "How many people are going to buy this?" and he said, "Well, only one. I am the only person that I know of at the moment who is interested in it," then on the basis of demand it would obviously be absurd to cater to this whim. But IRS didn't use this as the basis for their decision. Instead, they asked themselves, "What is the merit of this proposal?" It is true that there was only one customer, but the research project was so successful and so useful for public policy and tax research the data were well worth making available. The IRS didn't do it merely because an outsider wanted it, and I am not suggesting that the data center be created to pander to outside interests, academic enterprises, or others. If the Government wants to run its own operation efficiently, it should at least study the merits of the matter and not ask merely how great is the demand in terms of the number of people wanting it.

Mr. GALLAGHER. I think the question is, How is it going to best serve the people, the citizen, and the taxpayer?

Mr. RUGGLES. But not individually.

Mr. GALLAGHER. Yes, individually, because I think you have to consider the cost-benefit ratio of what good this will do against what harm it will cause to the individual citizen.

Mr. RUGGLES. That is correct. With that I agree, but by "individually" I guess I wasn't speaking of the same thing. You should not ask how many people want this particular data, or how much will each individual asking for the data directly benefit from it, or even how many times will individuals use the data.

Mr. GALLAGHER. It could be potentially harmful to a great many individuals. I think it would be essential to establish just what would be the uses that this would serve.

Mr. RUGGLES. I would agree completely.

Mr. GALLAGHER. Has anybody given this any consideration, Mr. Dunn?

Mr. DUNN. Let me add a few comments on this matter of the uses. First, of all, I don't think there is really any way, as a matter of practical possibilities, to determine something that we might call the request incidence or frequency of requests upon statistical files in the Federal Government, and certainly no way of identifying specifically what they would be upon an improved service and capability of this kind.

Now, one of the principal reasons why this is so is because most of the distribution of the information which is generated by this process is undertaken through published documents like the Census Monograph, and so forth. These documents go out to all sorts of places, including standard library, reference, and referral services of various kinds. People come to these records and documents for all sorts of reasons without any way of ever tracing who tried to get into the record for what, you see, for what purpose. Here is the important thing.

Well, let me make another comment on the same point and that is this: To try to anticipate what the frequency of requests would be upon a system which would improve the service and capabilities of matching records in various ways and so forth is likewise impossible at the present time because it would be roughly identical with the kind of problems DuPont would face when trying to decide whether to produce nylon or not.

Mr. GALLAGHER. Not exactly. We already have data centers set up. I think you should determine what use is made of this information at this point.

Mr. DUNN. No, there is a distinction here and it is a very difficult distinction to convey and I am not sure I can be successful in conveying this point. May I take a few minutes to try to convey this and do it in terms of a simple kind of example?

Mr. GALLAGHER. Please do.

Mr. DUNN. I would like to start, first of all, from the point of view that is very fundamental here in the whole operation of using numbers for analysis in statistics, and so forth, and that is that no number will convey any information to anyone, without being associated with some other number, except as it can be related to other numbers and except as it can be identified with an attribute or characteristic of that number.

Let me illustrate: Suppose I were to write on the wall over here the symbol "2" and ask you what it means to you. You would probably say nothing. You might try to give it significance by saying that it is a number in an array of numbers that falls between 1 and 3, but if you would say that, you are already trying to associate it with some other number, you see. However, if you are really quick, you will immediately say "two what?"

Mr. HORTON. \$2 million for this system. That is what I thought the minute you said it.

Mr. DUNN. It might be that, but if I said "two apples," the information content jumps immediately. If I go on and associate the apples with the behavior of people and say two apples are eaten by the average person each week, the information takes another jump. If I

associate it with something else and say this compares with the per capita consumption of three oranges per week, the information takes another big jump. If I go further and say in spite of this national average, northerners eat more apples than oranges, then the information content jumps again.

Mr. GALLAGHER. Less acid.

Mr. DUNN. That is a ridiculous example in a way, but what I am trying to point out here is, a task of statistical analysis or any kind of analysis—and there is the backbone for policy administration—is a way of associating records or numbers that have attributes to private enterprise, governmental units and so forth. Unless you can start with this kind of information, you don't have any information. You don't have anything that tells you anything. It simply cannot be done without the basic building blocks which ultimately are responding units of some sort. The building blocks must exist because there is literally no way that you can generate a statistic without them.

If you think you can solve this problem by abolishing the building block and leaving some kind of residue of statistics, you are mistaken because in the process you destroy the basis for all statistics.

Now, let me qualify this—

Mr. HORTON. I think you have just indicated why we are very concerned about this.

Mr. DUNN. Precisely, and I am concerned about this too. I am just as concerned as you are. The basic reason I am concerned you see is, the kind of system we are talking about here that can be of service to the public decision process cannot operate—I emphasize “cannot operate”—unless it will protect personal privacy and security successfully.

Mr. ROSENTHAL. Mr. Dunn, following that point up, you have made much ado about the fact that we have operated successfully in the Census, and the information contained therein by the Bureau is rather inviolate and yet I have just checked the statute and it says:

The Secretary may, upon a written request, and in his discretion, furnish the Governors of States and territories, courts of record and individuals data for genealogical and other proper purposes from the population, agriculture, and housing schedules prepared under the authority of subchapter (2) of chapter V.

Were you aware of the fact that that information can be given out by the Secretary and that he has that discretion?

Mr. DUNN. I am not an expert on the legal provisions here. With your permission, Mr. Chairman, I would like to come back to the earlier point in a moment.

Mr. GALLAGHER. Could you respond to that parenthetically and then we can get back.

Mr. DUNN. I am sure there are hierarchies of legal provisions here and some overrule others.

Mr. ROSENTHAL. This is the only exception to the other limitations that the Secretary has placed upon him. These are exceptions.

Mr. DUNN. I know of no instance in which the census materials have been used—no other instance where it has been used as basically an information-retrieval device about information on an individual, except in the case of genealogical records and there, bear in mind, this is the individual requesting information about himself.

Mr. ROSENTHAL. That is not what the statute permits. It permits much more than that and the thing that distresses me is that it may

well be that the men we have in charge of the Bureau now are concerned about these things, but the fellow in the line after him may not be at all concerned about it and may disseminate the material and in a very unwise, abusive fashion.

Mr. DUNN. There is no point of difference between us at all on this point.

I made the point in my statement that I think we have had enough experience with the various kinds of technical and legal devices for protecting security, and they have worked sufficiently well that we know it can be done. We have demonstrated that it can be done.

I am not taking the position that all of the legal and technical provisions which have been in effect for all of the elements and fragments of the Federal statistical system have been adequate in their functioning, have been adequate for this purpose. I am saying that we have a base of experience which assures us that we can go on to review substantive process, technical process and legal constraint to assure that a statistical system can operate with proper safeguards and I would suggest nothing be done without that kind of assurance being generated in the process.

Mr. ROSENTHAL. That is the point I want to make.

You would agree with the testimony we had this morning that before Congress authorized the executive branch or appropriated funds for the executive branch to institute such an installation that Congress make sure there is adequate legislation to protect the constitutional rights of the individual.

Mr. DUNN. Precisely.

I am on record within the Bureau of the Budget, in the Director's office, with a statement to the effect, in writing, that before a formal proposal can be developed in terms of the substance of a system that would be proposed for implementation, that a very substantial amount of technical and legal staff work needs to be undertaken and to be accomplished, and that the first step is essentially something comparable to what the engineers in the Pentagon might call a "phase zero" study. We have to look at this first with the kind of resources which allow us to say "Here's what we want to do: Namely, provide for more efficient statistical services—and at the same time assure and strengthen—and I emphasize "strengthen"—"the protections against personal privacy, and here is what it is going to take to fulfill these obligations."

Mr. ROSENTHAL. It seems to me that you fellows don't come in with clean hands if you hadn't considered that before you went to the trouble of printing all these documents and making this presentation. It would seem to me that that would be one of the first things I would have thought of before I went so far along as you people have. What you are doing now is reacting to the interest of a congressional committee. I have some doubts as to whether you would have done this had this inquiry not been held. It would seem to me your reputation would have been enhanced had you done this in the first instance on your own, of your own volition, and included it in all these documents, and books that you have prepared.

Mr. DUNN. I agree. I can only say in my defense in this regard two things: The first is—and this is really the only important point—that I was asked to come in and to review a series of procedural and

technical processes that are operating within the Federal Government as statistical services. They had nothing to do whatsoever with intelligence services of any kind, with dossiers, with any kind of system that would generate any information about an individual.

As a matter of fact, so far as I knew, this was a preliminary kind of a report for purposes of opening up the question for discussion, internal to the Bureau. I am not saying by that that it is inappropriate for documents to be released. I think it is perfectly healthy for the discussion to get out and in this kind of form. I welcome this and I applaud the work of the committee in this regard.

The only reason I didn't make a great issue over the personal privacy issue in the report was basically because I was operating within a frame of orientation which said we are talking about the way in which we improve a set of established statistical services, and we are essentially operating within a tradition where we just take for granted that we have got to protect the personal—

Mr. ROSENTHAL. I didn't mean to go into any narrow personal vein discussing these things, but apparently no one in the executive branch wanted to assume that responsibility and everyone wants to feel that they themselves are statistical technicians and their assignment was to stay within that particular role. As I see it, you can't have one without the other.

Mr. KRUEGER. If I may respond to this point, in examining this whole question, if we are subject to any dereliction at all, I guess it has stemmed from the basic tradition which we consider to be firmly established in the functioning of the entire Federal statistical system that the confidentiality of information reported to the Federal Government for statistical purposes must remain violate no matter what.

Mr. DUNN. Without it we have no system.

Mr. GALLAGHER. With that I agree, and I am happy to hear you say that, but one of the things we found in the confidentiality question business is that everybody seemed to take for granted that someone else will protect the confidentiality aspects and all of the people who draw a test of it feel that the judgment will be made at the Bureau of the Budget.

Now, I don't know how the Bureau of the Budget really got into the business of becoming the public conscience for truth and personality questions, yet they are the final authority on what is a good question to ask and what is a bad question, or whether or not a person's rights are being violated.

I don't know how the Bureau of the Budget got into this business.

Here we are once again taking for granted that the Bureau of the Budget will protect confidentiality. This is one of the problems that concerns us and I am very happy to hear all of you respond to what is a really serious problem to all of us.

Mr. DUNN. It is a problem to us.

Mr. GALLAGHER. But everybody takes for granted somebody else on the executive level will watch out as far as this problem is concerned. This is one of the problems and it is why we are in an era of corrosion of the individual's privacy. Ours is a very large Government and everybody else in the Government feels somebody else will watch out for this problem and this committee found there is not too great a concern for this, nor is there a center of interest where this specific problem is reviewed as to the interests of the individual citizen.

I don't think the Bureau of the Budget is properly geared for it. I understand they have 10,000 plus or minus questionnaires down there somebody is reviewing.

Mr. KRUEGER. It is a matter of record, as a matter of fact, in the hearings before the Supreme Court, in the case which Mr. Bowman referred to this morning, and it is in the decision of the Supreme Court where they took note of the concern of the Bureau of the Budget with this very problem.

Mr. GALLAGHER. I know you are concerned. The problem is I don't know whether this is where the jurisdiction rightfully belongs—to have everybody in the Government dump their problem into your lap and hope you will have the personnel to properly review it.

(Brief recess.)

Mr. GALLAGHER. The committee will come to order.

Mr. Rosenthal, being farther down the alphabet, will be here in a minute. If we could resume, it is your recommendations, in which we agree, that the safeguards that you have outlined here this afternoon be built into any program that will come forward as a result of the proposal?

Mr. DUNN. Very definitely. I would amend your statement only to say safeguards of this type, and to emphasize that we need in the process of designing such a program or system before its recommendation for implementation, to undertake staff studies which will pin down much more precisely the legal safeguards and modifications that might be desirable and required, and so forth.

Mr. GALLAGHER. What do you think of the proposal that I advanced on behalf of the committee this morning, of submitting your proposal to a further study with regard to the question of privacy and adequate safeguards?

Mr. DUNN. I think this would be a very productive effort, particularly insofar as the design of the legal protections is concerned and their appropriateness to achieve the objective in law that is desired. I would say, however, there are also some issues of information organization and production of substance here on which people of this type would not have a great deal to offer, and might easily misunderstand or confuse in some way, and would result in legal recommendations that were not effectively addressed to the control that was desired or legal provisions that inadvertently destroyed some essential technical characteristic of an operating statistical system. It seems to me both types have to work together.

Mr. GALLAGHER. We would get some Yale men.

It has been our suggestion that the refining process or the sifting process should be gone through before it becomes a hard proposal; that it go through a further committee which would not necessarily be opposed to the idea, but which would see that adequate legal requirements are built into the system, and that such a second committee of this sort be allowed to look at it from that standpoint.

Mr. DUNN. Are you asking me to recommend—

Mr. GALLAGHER. No. I said would you agree with such a recommendation and that it was necessary?

Mr. DUNN. I would not want in advance to state that one specific way of accomplishing this result or another is preferable, whether another review committee or through some kind of staff procedure or

what. I have not given any thought to this particular matter. I think it should be accomplished in some way, and this is something that should be considered very seriously.

In this connection, I want to make the point that while I functioned as a consultant to the Bureau of the Budget in generating this review, I am not currently a consultant to the Bureau of the Budget, and I appear here as a private citizen.

Mr. GALLAGHER. Yes. We appreciate your appearance.

Mr. DUNN. I present my views as a private citizen. I am not in a position to say that the Bureau of the Budget is or will or should follow these procedures in any official capacity as a consultant.

I would hope, however, the committee would not assume the fact I am no longer a consultant to the Bureau of the Budget is a reflection—

Mr. GALLAGHER. You have stirred up a lot of waves here already.

Mr. CORNISH. I think the chairman's suggestion this morning was when the Kaysen Committee had finished its work, that report be submitted to a panel of experts in constitutional law, and also in the fields of public policy that we have been discussing here this afternoon, to examine it strictly from that standpoint and to make some suggestions and comment on it so the Bureau of the Budget will have those views at hand when it makes its final decisions on whether to go ahead with this project and how it will do so.

Mr. DUNN. I am not sure I would want to say I have any firm opinion at the moment as to whether or not it would be appropriate to make the decision immediately following the submission of the Kaysen Committee report, or whether it might more appropriately and constructively come after the Bureau of the Budget had had time to do some additional staff work and to indulge in some internal thinking-out process following the Kaysen Committee report. I have the suspicion maybe the latter might be more productive.

Mr. CORNISH. In the course of the timing, certainly it should be before the center actually would be adopted as a firm proposal. I do not know exactly at what stage it might be, but certainly before that.

Mr. GALLAGHER. Mr. Dunn, we have now determined that it would be necessary to have some individual identification to a statistic; therefore, to a group of statistics. Each statistic must in some way be related back to a person, symbol, number, or name.

I would like to ask you one other question: You say this system is not an intelligence system. Would it be mechanically possible or impossible for this system to take on the characteristics of an intelligence system as the byproduct of a statistical system?

Mr. DUNN. I would like to answer that in the following way: First of all, I should like to give your concern in your question maximum support. As a matter of pure logic or philosophical premise, it is obvious that there is no system that can be designed by man that cannot also at least logically or conceptually be broken by man. To make any statement or take any position to the contrary is foolish. It cannot be demonstrated.

I am saying that I think we have accumulated in the area of statistical systems a very substantial experience with legal constraints and regulations and with procedures and practices that have worked, as a matter of fact, very well in protecting personal privacy in sta-

tistical systems; that having had this experience, we know these kinds of things can be made to work and we know these kinds of things can be extended in a number of ways and, as a matter of fact, strengthened through the application of the computer, that is, bringing the computer into the control process itself.

In the end, one simply has to say that we live in a system of law. Unless we have confidence that we can make a system of law work, we just do not have any recourse to anything.

Mr. GALLAGHER. Our system of law is conceived on a system of checks and balances. Are we not bringing about a vast imbalance here, and will we not have to rely on benevolent people using this for benevolent purposes?

Mr. DUNN. I do not think so.

Mr. GALLAGHER. Are we not creating the capability or are we not creating an instrument that can bring great imbalance? Suppose you had a nonbenevolent group in charge of a data center and then we threw Larry O'Brien's book on how to win elections into the computer, and then started to assimilate files on the 100,000 most likely delegates at the next convention. We would come out with some pretty interesting profiles and statistics, would we not?

Mr. DUNN. This is a complex question. There are several questions, as a matter of fact.

Mr. GALLAGHER. It is a complex issue. I am reducing it to a very simple political question.

Mr. DUNN. Let me answer in this way: First of all, I would agree with the statement Mr. Bowman made at the close of his testimony this morning. I think it quite appropriate and desirable that we not only think about controls upon the output, what can go out of the system. Here the basic notion is that no data about any individual can be released for any purpose—

Mr. GALLAGHER. Let us not talk about releases. Let us assume that it cannot be released.

Mr. DUNN. The other thing that is very desirable and necessary is to think about what kind of things it is legitimate to put into a statistical system. This is, I think, a matter of considerable interest and concern, and is another thing that needs to be thought very much about. Statistical systems as a matter of fact have never characteristically had very much information in them of a personal character, about the sex life of the individual or psychiatric interviews or things of that kind.

Mr. GALLAGHER. If you put in the MMPI—

Mr. DUNN. I am not sure I know what that is.

Mr. GALLAGHER. Minnesota Multiphasic Personality Inventory, which has a complete listing of your sex life, your religious beliefs, whether you love your wife or who you like to look at a movie with—all of this sort of thing. If you start programing that in the interest of statistics and press the button, you would have all the information you said would not be available.

Mr. DUNN. If it is not socially desirable to put this in, keep it out.

Mr. GALLAGHER. It is socially desirable. Otherwise, why did the Bureau of the Budget up until recently approve it as a test?

Mr. KRUEGER. We have never claimed specifically it would be socially desirable to put that particular kind of information into a data center.

Mr. GALLAGHER. Why would you use it in the first place?

Mr. KRUEGER. Someone had a very legitimate and important use for the information.

Mr. GALLAGHER. Then it is not impossible to think that someone would think it would be a very important use if we gathered up all of the people who took the MMPI and accumulated some statistics about how many people are happy with their wives or whether they believe in the second coming of Christ.

A lot of people do not believe in the first, so they are going to be discriminated against automatically by the computer.

Mr. KRUEGER. This is the importance of the question which needs to be given further consideration—what kinds of data should go into a center in the first place.

Mr. GALLAGHER. Yes, this is a very essential question, I should think.

Mr. DUNN. There is an additional point here, Mr. Chairman, which I think is worth some attention which has not come out in the discussion thus far, I believe. You have the data that are in there. Let us start with the assumption it is hedged about with all kinds of protection, procedurally and legal.

Mr. GALLAGHER. This is the 9,000 reels?

Mr. DUNN. No. The 9,000 reels, if I may, I would like to come back to, because there is a specific response on that which was not handled this morning, but that is not germane here.

You have data in the information system. In the first place, it is restricted data, restricted not only in terms of its availability but in terms of the kind of data you have in it. Let us even assume you have stuff in there that someone would like to get at. He has some motive for breaking the system, if I may put it in these crude terms. The simple truth of the matter is that it is just not going to pay him to try to break the system, quite apart from whether or not it could be done. Why? Because what has he got to do? He has to break the law. The penalties can be severe. He has to induce some key group of people, and maybe some of them are responsible to both Congress and the administration, or something of this kind, under the new procedures. They are going to break the law and violate their function.

After he goes through all of this, not only breaking the law himself but having a whole series of very impossible and improbable kinds of people to break the law, what is he confronted with? What is it that he wants? He wants some data about an individual. Why would he go to all this trouble and then, after he had gone through this kind of beltline or chain process, get to a file of several million records which must be searched through for this information?

Bear in mind, for statistical purposes this information is probably not organized with all of the data about the individual in one place. It is scattered all through the system, because that is the efficient way to organize, the format of data for statistical purposes, not the efficient way for intelligence purposes, but the efficient way for statistical purposes. He has to go through all this. If what he wants is a little bit of information about one individual or even a few individuals, it is much less risky and much more economical for him to go out and find out for himself, hire a private detective or drive by the guy's house—

Mr. GALLAGHER. He can do that now, but when you are centralizing, you are reducing the cost and increasing the risk.

Mr. DUNN. No. Presumably—

Mr. GALLAGHER. You just told me this could be converted into an intelligence system.

Mr. DUNN. Not if it is protected by law, and even then it would be a very costly thing. It would be a very improbable kind of thing to do.

Mr. GALLAGHER. Would it not be more costly to build in safeguards?

Mr. DUNN. I am talking about the safeguards. I am assuming the safeguards. I am not questioning the safeguards. I am saying we have to have those. I assume that you were raising the question, even assuming we have a protected system, don't you have a system where the stakes for getting into the system are not so high that safeguards might be brought into the system? I am responding and saying conceptually there is no system that cannot be broken, but if you have a system that is safeguarded appropriately, the cost of trying to break the system is astronomically beyond the value of getting an individual piece of data which could be much more economically and much less riskily gotten in some other way if what you want is some data about an individual.

You see, it just does not make sense to try to go into some great big file or record—for me, for example, if I wanted to find out something about Paul Krueger, to go into some big file or record where some limited number of characteristics, which might not be the ones I am interested in, are included with millions of other records, and try to prostitute a lot of people in the process, to find that out, when the chances are by hiring a private detective or going around and snooping a little bit myself or talking to a few of his friends I could find out practically all the things I want to know about him anyway.

Mr. HORTON. May I ask a question at this point, Mr. Chairman?

I think you have been here and heard Mr. Macy's article referred to in which he, the head of the Civil Service Commission, talks about the wonders of this new system and says that direct tape-to-tape feeding of data from one department to another may become common. Then he goes on to say how they have used this computerized file to get names to furnish to the President for candidates for presidential appointments. So they are already using this system.

Mr. DUNN. No, sir. May I make a correction? They are not using this system or any system like it. This is not a statistical system. It is an intelligence system. In my testimony I made a clear distinction and said I am not talking about that.

Mr. HORTON. You were talking about getting some information on Mr. Krueger.

Mr. DUNN. What I was saying is if I wanted to try to use a statistical system for intelligence purposes, it would be a very inefficient way to try to get intelligence.

Mr. HORTON. But you could do it. It is on the tape.

Mr. DUNN. You might be able to do it by breaking the law and getting six other people to break the law.

Mr. HORTON. We do not have any law on that now.

Mr. DUNN. I am saying you do not establish it until you do have.

Mr. HORTON. Could I ask a couple of questions, Mr. Chairman?

Mr. GALLAGHER. Mr. Horton.

Mr. HORTON. In this report of yours, Report No. 6, of December 1965, there is an appendix B which is referred to on page 6. You sug-

gest, under existing authorities, to begin work on these 9,000 tape nucleus archives identified in appendix B. I am not sure whose report appendix B is. Is this your report?

Mr. DUNN. It is my report; yes, sir.

Mr. HORTON. Appendix B is your report?

Mr. DUNN. No, sir; appendix B is not my report. That was produced by a gentleman from the Bureau of Labor Statistics by the name of Mr. Mendelsohn, who was on loan to the Office of Statistical Standards for the purpose of making this review at that time.

Mr. HORTON. He was working for you?

Mr. DUNN. That is correct.

Mr. HORTON. You adopted this appendix B?

Mr. DUNN. That is correct.

Mr. HORTON. As your report?

Mr. DUNN. That is correct.

Mr. HORTON. You went over it very carefully, I am sure.

Mr. DUNN. That is correct.

Mr. HORTON. In the report you talk about data bank requirements, and you talk about getting all these various reels that are now out in the other agencies, into this central statistical center.

Mr. DUNN. May I comment on that, because this is the 9,000-reel issue that was mentioned earlier, to clarify this point, because there is confusion residing on this point?

In my report I identify a number of functional areas in which some improvements in efficiency are useful and required. Many of these functional areas do not introduce anything new insofar as the issue of personal privacy is concerned. One of the areas that I was talking about in this area was the problem of archives. This was the fact that there exists at the present time within the Federal Government no established set of procedures or standards for determining what records in the agencies will be archived; that is, preserved in ways that can be used subsequently, nor any institutional means nor any standard funding process for seeing that they are protected.

One of the very serious problems we have had for some time is the fact that many very useful records are being destroyed inadvertently or unnecessarily.

Mr. HORTON. Wait a minute, Mr. Dunn. We do not have all night here on this—I wish we did have—to go over all this information. It says:

Data bank requirements. An estimated \$3 million to \$3.5 million and 3 to 5 years are needed to stock the proposed data center with Federal statistics now in existence.

You are not talking about any archives. You are talking about stocking the system. Then you say:

These data will probably comprise about 20,000 reels of magnetic tape. However, a Federal center could be stocked with a respectable volume and variety of data relatively quickly for about \$260,000 at the rate of about \$27 per reel. A bank of 9,000 tape files could be established in about a year. Such a course would provide a fairly representative selection of significant data including, for example, 750 reels of the Census housing data.

You are not talking about archives there, are you?

Mr. DUNN. Yes, sir. My language may not communicate it effectively, and I shall take the blame for that, but what basically was intended there, what we were talking about, was not the matter that we

would take some reels immediately and, without any previous authorization or any review of this process, set up a data center which would perform all these integrated functions. The thing which we had in mind there was that there is a tremendous amount of spoilage taking place in existing records because we do not have procedures for preserving them, and that very simply, within existing authorities and procedures, we could start with 9,000 reels or some specified number of reels—I do not remember the detail now—and put them under some provision that would assure they would be preserved and protected for future use, safeguarding them.

Mr. HORTON. That is not the substance of this appendix B. The substance here is to build up a library for the data bank. That is the basis of it.

Mr. DUNN. The other function—

Mr. HORTON. Now let me read you something else on page 3 of that appendix:

Agency representatives seems excessively concerned with the confidentiality question. Turning data over to a Federal center would be a breach of contract with respondents who have been assured that none but agency personnel would view their reports, it was said. I tried to convey the assurance that if a data center were established it would assume the obligation of protecting both the agency and the respondent. Since feelings on this matter run quite deep, some steps should be taken at the outset to vitiate them or discussions beyond this narrow consideration could founder. One constructive suggestion was made in regard to confidentiality. Mr. Robert Mencke, of the Securities and Exchange Commission, expressed the view that corporate concern dealt mainly with current affairs. It was his feeling that after a period of 5 to 10 years back, data could be exposed to public view without serious objection by respondents. There would be difficulty, perhaps, in applying such a rule retroactively, but a notice to this effect on future collections of data might serve to make the problem less troublesome in the years ahead.

How do you explain that?

Mr. DUNN. This is a report of a man who went out to interview the agencies and get their reactions, and he is reporting on their reactions. The reactions to me seemed to be perfectly sensible.

Mr. HORTON. You adopted this, you told me in the beginning. I asked you if you adopted that statement, and you said you did, and you put it in this report.

Mr. DUNN. Let me correct myself. I do not imply that any or all of the things suggested in the appendixes were included in the substance of my recommendations.

Mr. HORTON. On page 6, under subdivision C, you say under existing authority to begin work on the 9,000 tape nucleus archives identified in appendix B.

Mr. DUNN. That was to protect them from being destroyed inadvertently, not with the purpose of initiating a system.

Mr. HORTON. Now moving to the next consideration, this is going to be on that tape, is it not?

Mr. DUNN. What is going to be on the tape?

Mr. HORTON. All this information that comes from these various agencies and some in the future.

Mr. DUNN. Whether they are all in there or not, I would presume is subject to the review process which would be a part of the system design which says what is legitimate to go into the system and what is not.

Mr. HORTON. You very carefully pointed out the distinction between an intelligence and a statistical system, and this is very fine. It sounds fine. But the question that I have to ask has to do with the basic distinction between the statistical system and the intelligence system, because it seems to me that a statistical system is the same thing basically as an intelligence system. You can get intelligence information off a statistical system, can you not?

Mr. DUNN. There are records about individuals and individual attributes in a statistical system. They have to be there in order for it to work. It cannot be used as an intelligence system if it is properly safeguarded, and I maintain it can be properly safeguarded.

Mr. HORTON. When you say "properly safeguarded," I do not know any law that is going to apply to a machine. You detailed on page 4 how the machine could be set up to do this and not to do that. It could be set up so you could get personal information on an individual at a push of a button, could it not?

Mr. DUNN. You can design intelligence systems, yes, that will retrieve information and even dossiers, if you like, on individuals. This can be done.

Mr. HORTON. This system that you are talking about. I want to know technically, not legally but technically, can this system be set up so it could be converted into an intelligence system?

Mr. DUNN. Any kind of system can be set up to perform any purpose, yes. I would say we are not setting one up for that purpose.

Mr. HORTON. I understand you are not setting it up for that purpose, but what I am concerned about is the fact that you will have available in one place all this information that comes from the Department of Defense, the OEO, the Civil Service Commission, the FBI, from wherever and whatever source you want. All these magnetic tapes will be put in there. That information will be fed in one way or another.

Mr. DUNN. Not unless you decide all these things are appropriate to put in this in the first place.

Mr. HORTON. Have you decided what is to be put in the system?

Mr. DUNN. No, sir. That is not my role or function.

Mr. HORTON. Did you recommend anything with regard to that?

Mr. DUNN. I did not.

Mr. HORTON. All you recommended was setting up the monster, if you will.

Mr. DUNN. Whether it is a monster or not depends upon whether it is properly safeguarded.

Mr. HORTON. You said it could be called that by a layman, and I adopt that suggestion of yours.

Mr. DUNN. It would be appropriate to call it that if it were so designed to perform in that way.

Mr. HORTON. It could get all this information in it.

Mr. DUNN. It could be designed to do that.

Mr. HORTON. It could on the push of a button get this personal information about an individual.

Mr. DUNN. It could be designed to do that, but then it would be an intelligence system and not a statistical system. I would assume the object of the whole exercise is to safeguard against that in terms of both the legal constraints which can be applied and the substantive

and procedural processes that can be applied, using, as a matter of fact, the computer as an aid in the security process.

Mr. HORTON. I am sure I am not an expert on how Government works, but I know how these things generally happen. You start off with a report like this, and then the first thing you know, something else happens. The first thing you know, you are getting this personal information. This is a report, and I realize that you are not responsible for the legal ramifications of what happens once you make the report. I appreciate the fact that you are no longer a consultant with the Federal Government.

But you have made a recommendation for a central data center that could get all this type of information I am talking about, and you do not define in here, at least in your report, as I see it, the difference between intelligence and statistical.

Mr. DUNN. That is precisely the point I admitted to Mr. Rosenthal earlier in the testimony this afternoon. I regret that.

Mr. HORTON. Your recommendations are not along those lines. Your recommendations have to do with a lot of other things. That is, on page 4: "Manage the Archives records, develop referral and reference services, provide explicit facilitating services for users." I do not know who the "users" are, but it continues: "including file arrangements, cross-tabulation, extending output options, obtain translations, file modification, record matching." Can you identify which of these is statistical and which is intelligence?

Mr. DUNN. All are statistical.

Mr. HORTON. All of them?

Mr. DUNN. Yes, sir.

Mr. HORTON. Every one of them?

Mr. DUNN. Yes, sir. There was no time in the preparation of my report, consideration of any part of it, that there was any intention to address ourselves to the issue of intelligence systems at all.

Mr. GALLAGHER. Would it not be a problem to address yourself to that problem, so that it was not built into this system?

Mr. DUNN. I beg your pardon?

Mr. GALLAGHER. Would it not have been advisable to address yourself to that system in order to prevent it from having the conversion possibilities of becoming an intelligence system?

Mr. DUNN. This is something that may very definitely need to be addressed in the process; yes, sir.

Mr. HORTON. That is all.

Mr. GALLAGHER. Mr. Ruggles, how close has the Kaysen report been watched?

Mr. RUGGLES. I honestly do not know.

Mr. GALLAGHER. You are a member?

Mr. RUGGLES. Yes, sir. Professor Kaysen has taken a new job and in the process of transferring from Harvard to the Institute for Advanced Study, he has, I think, been somewhat busy and the committee has not met for a final time. The report is still in draft.

Mr. GALLAGHER. Tell him that he has overwhelmed the Congress up to now.

Mr. HORTON. Mr. Chairman, I did want to ask one question.

Mr. GALLAGHER. Yes.

Mr. HORTON. Mr. Ruggles, you are a member of this Research Council, Social Science Research?

Mr. RUGGLES. No, I am not.

Mr. HORTON. You work for them, is that it?

Mr. RUGGLES. No; the way the SSRC report came about, was that the American Economic Association requested the Social Science Research Council to undertake a study of the problem of the preservation and use of economic data.

I was asked by the Social Science Research Council if I would chair a committee to study the problem. This committee studied the problem for 3 to 4 years, conferring with the various government agencies and so on, and after that time brought out a report.

Mr. HORTON. That was the so-called Ruggles report?

Mr. RUGGLES. That is correct.

Mr. HORTON. The council is a private organization, is it not?

Mr. RUGGLES. Yes.

Mr. HORTON. Would the members be users of this type of information?

Mr. RUGGLES. No, they would not.

Mr. HORTON. They would not have any call on it?

Mr. RUGGLES. No interest or function.

Mr. HORTON. Do they call on the Federal Government now for any of these services?

Mr. RUGGLES. No, I would not be able to testify on this because I know nothing of their finances. I think they are mainly supported by Rockefeller and Ford and other foundations.

Mr. HORTON. I was thinking in terms of statistical information.

Mr. RUGGLES. No, they do not do any research work whatsoever.

Mr. GALLAGHER. I think you brought out before that grantees of that organization would make use of it.

Mr. RUGGLES. The SSRC gives scholarships and fellowships to scholars. It is like the other foundations and research groups that give away money.

Mr. HORTON. The grantees may be users of that information?

Mr. RUGGLES. That is right. In another connection, my wife and I are doing a Social Science Research Council Project at the Census Bureau on price-cost behavior of manufacturing establishments. This study is done under elaborate safeguards of disclosure, you will be happy to learn.

Mr. GALLAGHER. I am.

Mr. RUGGLES. In our research we never see the individual firm or establishment data. Nevertheless, the computer was used on establishment data for the first time in 1954. Methods were devised on the computer to match the individual establishment records to provide a continuous report for the same establishment for a period of time.

The purpose of this project was to study, for producers as a group, whether in a period of high demand, producers tend to raise prices more than their costs, or whether they tend to narrow their margins and are squeezed. This is important for problems of fiscal policy in the Nation, in worrying about how to dampen a boom, the rule of wage-price guidelines, and so on. There is currently a lot of interest in this sort of question. Although we are not interested in the individual establishment we had to get data for each establishment so that we could see how on an average they all behaved. This is the sort of work which the Social Science Research Council, together with the Census

Bureau, sponsored in a series of six or seven major monographs that attempted to utilize census materials for academic research. The money originally came from the Ford Foundation. This is a typical sort of thing they undertake.

Mr. HORTON. In your initial studies did you try to differentiate between this classification that Mr. Dunn has come up with now of today here, this intelligence system, and statistical system approach?

Mr. RUGGLES. No. We were very much aware of the problem of individual disclosure. This, as a matter of fact, was very, very evident to the committee right from the start and we did emphasize in the SSRC report that proper disclosure safeguards had to be provided.

Mr. HORTON. With this statistical system that has been described by Mr. Dunn, does it not have for all practical purposes the intelligence system built into it? All the information that is there is related to an individual; is it not?

Mr. RUGGLES. Yes, sir. I would say that what you point out is quite correct. There are really two ways of subverting this system. I worry about this and I think you do have to build safeguards. One way is, of course as you suggest, that instead of a benevolent group in charge you get somebody in who is not interested in the public good and he uses it for private purposes. We have to worry about this whenever we appoint a Secretary of Treasury, or whenever we appoint an Attorney General, or whenever any of these major appointments have been made.

Mr. HORTON. Excuse me for interrupting. I am worried about that but I am—

Mr. RUGGLES. You should be.

Mr. HORTON. I am also equally worried and more so worried about 5 or 10 years from now.

Mr. RUGGLES. That is right.

Mr. HORTON. The bureaucrat, as Mr. Packard described him yesterday, for the sake of efficiency and for recommendations to short circuit the different problems that he might be up against says "it is important for us to have this information. There might be a good reason for it."

Mr. RUGGLES. This is the same thing.

Mr. HORTON. I am so happy we have one of these banks. I think it is wonderful. This is certainly the type of information we need.

The point I am trying to make is this: I may very well in 5 years from now say this is fine and this information ought to be made available. What happens to the private individual citizen and his rights involved in that? That is the point I am trying to make. This does put this information into a central system and one of the points that has been made throughout our hearings has been that by having this information dispersed—birth certificates in one place, military records someplace else, and bank statements someplace else, it is somewhat safeguarded.

As a Member of Congress I am sure that the Government has some information on me about money that I have received or statements that I have made in connection with campaigns. All this is in different places at the present time. Now what we are proposing is to make it available in one central place where we can, regardless of how many safeguards we have, set the system up technically so that with the push of one button a card will come up and give all this information. That is accurate, is it not?

Maybe I have not covered all of it but that is possible, is it not?
 Mr. RUGGLES. I do not think it is really possible to bring all those records together. If you want my frank opinion, I think that is just dreaming.

Mr. GALLAGHER. David Sarnoff said in his article that by 1976 a computer will be capable of making 400 trillion computations an hour, or 2 billion computations per hour for every man, woman, and child. (The article appears in app. 3, p. 298.)

Mr. RUGGLES. You do have dangers in the system and they are present. I think we have to concern ourselves with them. We have now Archives. Archives is a general central system. You have to realize this. They have under their direction and their control all of the IRS records. They have all of the presidential papers of Kennedy, Eisenhower, all of these people. They have all of the basic documents of the United States under their control. You are quite right. It is possible for these to be subverted. It may be that Archives should be broken up and we should decentralize it.

Mr. HORTON. But it might be possible, would it not, that it would be subverted, but for good purposes it could be made available. That is what I am concerned about also.

Mr. RUGGLES. That is right. I think that we have to worry about this and ask whether centralization of many of our functions is at all useful. I know the Congress worries about this a great deal. Perhaps we have too much Federal Government. I do not know.

Maybe even many of the powers that the Federal Government has should be broken up. For instance, maybe we should not have a single tax system.

Mr. HORTON. You are getting into something else.

Mr. RUGGLES. No, it is the same sort of thing.

Mr. HORTON. We are talking—

Mr. RUGGLES. Centralization brings power.

Mr. HORTON. We are talking about the preserving of the right of privacy of an individual and making it impossible for all of the information on him to be made available on just a snap of a finger. That is what we are trying to do. We want to safeguard him as best we can in this computerized jungle that he lives in at the present time.

Mr. RUGGLES. If what you are asking is, should we bring all the information from all agencies about every individual together, I would put an emphatic "No" to that. Then does it follow that we should make sure that no information about any individual ever gets together anywhere?

My answer to that would be "No." Obviously, the best position is somewhere in between. We do want to build these major economic statistics systems.

Mr. GALLAGHER. Mr. Horton's concern parallels the concern that you yourself in your statement point out:

One of the most encouraging developments of recent years has been the increasing recognition that information obtained illegally does not constitute proper evidence, and that certain agencies of the Federal Government itself may have acted illegally in their attempts to procure such information. Thus wire-tapping, improper seizure of records, etc., are now considered illegal in situations other than those directly concerned with national security.

Mr. RUGGLES. That is correct.

Mr. GALLAGHER. You recognize the fact that within the Federal Government, sometimes its enforcers do act illegally to obtain this information?

Mr. RUGGLES. That is right.

Mr. GALLAGHER. You have rightly stated that the courts have thrown this out. But on the other hand, we have all sorts of little cute devices now in the enforcing area where you can use illegal information and not admit where you get it, and not admit it as evidence, but under the broadening immunity statutes you can put somebody in jail forever, or to carry this to its logical conclusion, well beyond the point of the crime for which he might be committed on civil contempt of court if he has not admitted to the information being obtained illegally.

All this ties in with some of the concern a lot of people feel and we could very easily drift into a police state where you do have corruptions at every level. I am very happy to read of your awareness of these very problems.

These are the concern of the subcommittee.

Gentlemen, on behalf of the committee I want to thank you very much for your appearance here and for your testimony and helping to air the problem a little more. You have made a real contribution to our understanding. With that, I want to thank you very much for being with us today.

Mr. DUNN. Thank you for giving us this privilege.

Mr. GALLAGHER. The committee stands adjourned until 10 a.m. tomorrow morning.

(Whereupon, at 4:30 p.m., the committee adjourned, to reconvene at 10 a.m. Thursday, July 28, 1966.)

THE HISTORY OF THE UNITED STATES

The history of the United States is a story of growth and change. It begins with the first settlers who came to the continent in search of a better life. They found a land of opportunity, but also a land of conflict. The struggle for independence was a long and hard one, but in the end, the people of the United States won their freedom and established a new nation. The years that followed were a time of great achievement and progress. The United States grew in size and power, and its influence spread across the world. The American dream became a reality for many people, and the United States became a model for other nations. Today, the United States is a powerful and influential country, and its history is a source of pride and inspiration for all Americans.

THE COMPUTER AND INVASION OF PRIVACY

THURSDAY, JULY 28, 1966

HOUSE OF REPRESENTATIVES,
SPECIAL SUBCOMMITTEE ON INVASION OF PRIVACY
OF THE COMMITTEE ON GOVERNMENT OPERATIONS,
Washington, D.C.

The subcommittee met, pursuant to recess, at 10:19 a.m., in room 2247, Rayburn Office Building, Hon. Cornelius E. Gallagher (chairman of the subcommittee) presiding.

Present: Representatives Cornelius E. Gallagher, Benjamin S. Rosenthal, and Frank Horton.

Also present: Norman G. Cornish, chief of special inquiry; Miles Q. Romney, associate general counsel, Committee on Government Operations; and John Forsyth, special minority consultant.

Mr. GALLAGHER. The subcommittee will come to order.

The first witness this morning is Mr. Paul Baran, computer expert with the Rand Corp. In the opinion of the Chair, he is one of the few persons in the United States acknowledged as an expert in the relationship between the development of computers and the invasion of privacy.

Mr. Baran has received his B.S. degree in electrical engineering from the Drexel Institute of Technology; M.S. in engineering at the University of California; and his M.S. thesis dealt with computer simulations as an aided adaptive printed character recognition scheme.

While at Rand, Mr. Baran has also served on several ad hoc Department of Defense committees and as a consultant to the Institute for Defense Analyses and the Stanford Research Institute. The Department of Defense panels include those on the communications network switching and survivability of command and control.

Mr. Baran is author of many papers in the field of computers and communications and has lectured at the University of Michigan on computers in real time. He is a member of the Association for Computing Machinery and a member of the Institute of Electrical & Electronic Engineers, including its professional groups on computers and communications systems technology.

The Chair welcomes you here this morning, Mr. Baran. Would you proceed?

STATEMENT OF PAUL BARAN, COMPUTER EXPERT WITH THE RAND CORP., SANTA MONICA, CALIF.

Mr. BARAN. Thank you, Mr. Chairman. I would first like to summarize my remarks and then delve more deeply into the reasons for my position. I do so in the role of the private citizen and not as a representative of the Rand Corp. or its sponsors.

I have been asked for my viewpoint on a centralized Federal data system, but I have broadened my response to direct attention to a larger issue: whether, in fact, we might not already be part way down the road building a system with all the obvious dangers of a single Federal data system, but without its clear visibility.

The problems of the invasion of privacy are, in my view, significant, and they will exist whether or not the central data bank is created by the Government. Individual data systems, both public and private, now being developed, can be tied together eventually into a network that will present essentially the same problems.

Every time someone proposes a system that handles embarrassing information, we are commonly reassured by the words, "Only those having a legitimate need to know will have access to the information." While the statement rings seductively of safety and is granted in good faith, its validity is sometimes overstated—particularly when such systems are interconnected. As one familiar with the inherent weaknesses of both our computer and communications systems, I am less sanguine about these assurances.

My remarks are intended to raise a healthy skepticism to this soothing sirup. While our computer and communications systems are fool-proof, they are not smart-proof. These systems are wide open to tampering by anyone sufficiently intelligent and motivated enough to take advantage of their weak spots.

My key suggestion is that we proceed slowly and cautiously to insure that proper safeguards are built into the systems from the outset. I do not propose delay as an obstructionist act, but only to allow the thought required to insure construction of the safety features required. But this takes time—and dollars. The full ramifications of the problem areas created are not yet well understood by the computer profession. And this is too important a decision to leave to any single computer manufacturer.

There is at present little financial incentive for any single computer system supplier to conceive and create new safeguards. Perhaps this may be attributed to the lack of sophistication of each individual user or perhaps no single user can demand extra new safeguards when almost comparable systems have been built in the past without such protection. I think it time that Government speak clearly as an advocate of the public interest in the future and initiate the improvements we desire. The first step would be to start considering some of the individual computer systems now being built from the viewpoint of subsystems of a larger, overall system now under growth.

The men guiding the computer companies, the ones who must perform the detailed work of building safer systems, in my experience are among the most public spirited and enlightened in the Nation. But I believe that they will get on with the job more rapidly once their attention has been directed to the long-range implications of their babies.

PREFACE

It is a privilege to be invited to express my thoughts on the future possibility of the inadvertent invasion of privacy by the computer. I am highly pleased but, I must confess, surprised by the rapidity with which Congress is addressing itself toward the examination of this subject—one not yet generally recognized as being a problem by most in the computer profession.

This subcommittee is considering a specific proposal: to build a larger centralized data base for the Nation to reduce the costs of duplication of files and to provide more rapidly available information to those with legitimate need. The initial goals are valid and useful. But of common concern is the range of possible side effects. In general, I wonder about the potential threat to our historic right to privacy that could be endangered by a lack of appreciation for the present-day limitations of the computer and communications technology that could allow tampering of files by a sophisticated criminal, or a conspiracy, or even Government itself.

The initial questions are those of examining the proposed central file system, considering its weak spots, and creating a precise description of those safeguards required that are technologically and economically feasible. If the gap is too great, then clearly we should not build the system. But as a practical matter we should realize that eventual development is almost inevitable. We would do well to concentrate on the more constructive and larger issue of: How shall we control the development of the automation of all sensitive information files in order to best protect the rights of the individual and avoid a "1984" nation?

This may sound pessimistic, but if one can save money automating a data system it is only a matter of time until it happens. The only questions are: When? and How? I would like to add the further distressing thought that we may already be well along in the creation of the very system whose needs and dangers we are discussing today. This might sound bizarre, but consider the following line of reasoning:

Our first railroads in the 1830's were short routes connecting local population centers. No one sat down and laid out a master plan for a network of railroad rails. With time, an increasing number of such separate local systems were built. A network gradually grew as economic pressure caused the new links to be built to span the gaps between the individual routes.

We didn't start to build a nationwide telegraph network in the late 1840's; only independent telegraph links. But it was not long before we had an integrated nationwide network. Even the name, Western Union, recalls the pattern of independent links joined together to provide a more useful system.

We didn't start to build a nationwide telephone system in the early days of the telephone in the 1890's. Yet, today we have a highly integrated telephone network.

Such patterns of growth are not accidents. Communications and transportation are services that historically tend to form "natural monopolies." The reason is well understood. It's cheaper to share use of a large entity than to build your own facilities. Hence, if you were to look at the earth, say, from the far-off vantage point of the moon, it would appear that the growth of these integrated networks out of individual pieces is almost biological.

So much for history. What is of concern to us is that automated information files have the same properties as communications and transportation that causes the integrated networks to be self-agglomerating. It is cheaper to share the information by tying together independent systems than by building a very large number of highly duplicating systems without interconnection. But "information" can be too

treacherous a commodity to be widely disseminated with ineffectual controls. Even a little information improperly used can do irrevocable harm. Information is readily counterfeited. It can be quickly reproduced and widely transmitted very cheaply.

Today we can see the independent, private automated information systems being interconnected to form larger growing systems. The direction of growth is clear.

My thesis is this: Today we are already building the bits and pieces of separate automated information systems in both the private and government sectors that so closely follow the pattern to the present integrated communications structure that a de facto version of the system you are now pondering is already into the construction phase. It is in many ways more dangerous than the single data bank now being considered.

There is no culprit. No one set out to build our system. It's like little Topsy in Uncle Tom's Cabin who said, "Never was born. I 'spect I grow'd."

Mr. ROSENTHAL. Is it your point that these pieces are just being independently developed by various agencies and various groups, and, all of a sudden, they will merge by alleged necessity?

Mr. BARAN. Yes. We see this with independent credit systems built to cover small areas and then they find it is economic to cross-connect. We see this with airline systems; systems built for individual airlines are interconnected to swap information back and forth to get people reservations on other systems.

Mr. ROSENTHAL. So, the point you make is that even though the Government has not put their stamp of approval on building this system it is growing on its own because various groups are independently developing its starting points.

Mr. BARAN. Precisely.

THE CHANGING COMPUTER

Once when we spoke about a computer we meant a large room full of equipment. It was used by scientists to perform complex calculations and by businessmen to prepare payrolls, store inventory data, and similar generally repetitive tasks.

Both the form and the uses of computers are now undergoing radical changes. They have become so powerful, can store so much data, and process this data so quickly that it becomes possible to "time-share" a simple computer. You will be hearing more of this word "time-sharing" in the future. Time sharing means literally that many people have access to the single computer installation. The computer has so much capability and is so fast that it creates the illusion that each user has his own computer.

Users time-sharing a computer need not be in the same room or even the same building. They can be hundreds or even thousands of miles away. All it takes is a telephone connection to a remote electric typewriter-like device. Early examples of such systems include the local stock brokerage "systems" and airline reservation systems. In one system, over 3,000 separate stockbrokers around the country can push a few buttons to display the latest prices on any selected stock. Making and checking an airline reservation in a matter of seconds is

is so common that we forget about the good old days of manual data processing as we sat interminably in a drafty airport waiting to find out whether a seat on a desired flight was open. Paradoxically, these words were written before the strike and today's weather.

r. GALLAGHER. I don't think this will be needed any more.

r. BARAN. Right. This paragraph is inappropriate.

RECORDKEEPING

Simple recordkeeping, a mark of a highly developed economy, has become a prime area of development of these large computer file/communications systems. Much routine clerical work has been transferred to computers interrogated by humans. More people will have access to these systems at even greater distances from the computers.

SOME INDIVIDUALLY USEFUL SYSTEMS

Today we see time-shared file systems used to store insurance records. In a fraction of a minute it is possible for a clerk in another part of the country to check to see if one insurance renewal check has arrived.

To date such systems seem to pose no overt social problem. The information handled is not highly sensitive, and access is generally limited. But as new uses are being found for time-shared computers, a subtle change is beginning to take place.

In New York State, experiments are underway with a new criminal information record system. A police car uses radio to transmit automobile license tags into a central computer. If there is an outstanding warrant, the information comes back so quickly that a second police car located slightly ahead is able to stop the suspect. Preliminary tests have shown the system to be highly effective. We are all familiar with credit-check systems which use our driver's license numbers when cashing checks. This system is so fast that bad-check artists have been caught redhanded.

Seemingly such systems make a socially useful contribution. But let us look into the future and consider what their uncontrolled proliferation could mean.

THE TRAIL OF RECORDS IN A CIVILIZED LIFE

As we pass through life we leave a trail of records, widely dispersed and generally inaccessible—except with a great deal of effort and diligence.

Beginning with a birth certificate, we continue to accumulate hospital and medical records. We become deductions on our parents' income tax. In school we generate records of our grades, attendance, IQ tests, personality profiles, et cetera. Automated teaching will add to this recordkeeping. The volume of data recorded per child may be expected to increase even more markedly. After school we start accumulating employment, social security, and selective service records. We may get a driver's license. Most of us will apply for marriage licenses, and some will collect divorce decrees which will end in voluminous court records. If we are lucky, we will be

able to avoid arrest and jail records. We move from job to job in a mobile economy creating moving-company inventory records for our goods. Even as we move from place to place we leave behind short records of our airplane reservations and for some reason every hotel makes a ritual of acquiring and preserving the alleged names and addresses of its guests for posterity.

Book clubs and magazine subscriptions reflect our point of view and interests.

This is only a partial list. Play the game yourself and think of all the records you leave as you go through life.

WHY SO MANY RECORDS?

Behind all this creating of records is the implicit assumption that they will some day be of use. In order to be of use, there must be some means of interrogating the files to resurrect the information sought. Thus, we envision large families of systems, each individually useful. For example, an Internal Revenue Department investigator might wish to have immediate access to the tax returns of each of the associates of a man who is being audited to check for consistency of financial relationships.

A company may wish to have rapid access to its personnel files to know whether to give a good reference to a former employee.

A doctor may wish to trace the entire medical history of a patient to provide better input into a diagnostic computer.

The Veterans' Administration may wish to examine a man's complete military record and possible other previous medical records to see whether the ailment claimed as being service connected really is.

A lawyer for the defense of a man will wish to search for jail and arrest records, and possible credit records of all witnesses for the plaintiff.

Professional licensing boards may want to delve into any records to determine if an applicant has an unblemished character.

The military, in filling extremely sensitive positions, may even wish a record of all books borrowed by a prospective applicant to insure that his interests are wholesome and he possesses the proper political bias desired.

ACCESS TO THIS INFORMATION

Today it is difficult to gather such information about a prospective examinee. If one went through direct channels and asked most sources for their records about a person, he would most likely be rejected, if for no other reason than that the information is not readily available—cheaply. Even if the records were publicly available, the investigator would have to spend a great deal of time and effort delving through to discover pertinent data. Today, as a practical matter, if an individual wishes to obtain certain information about a person, he hires a private detective who charges a great deal of money and expends a great amount of time obtaining a little information from a portion of these potential records. The price for a fishing expedition for information is high and most of the fish are inaccessible.

THE IMPENDING PROBLEM

So much for the pleasant past. Consider the following argument: A multiplicity of large, remote-access computer systems, if interconnected, can pose the danger of loss of the individual's right to privacy—as we know it today.

The composite information data base may be so large and so easily accessible that it would permit unscrupulous individuals to use this information for unlawful means.

Modern organized crime should be expected to have the financial resources and access to the skills necessary to acquire and misuse the information in some of the systems now being considered.

We are concerned not only with the creation of simple "automated blackmail machines" using this information, but with the added implication of new powerful "inferential relational retrieval" techniques now being developed. Such techniques, when fully refined, could determine relationships of any person, organization, event, et cetera, to any other person, organization, or event.

Human beings, by their day-to-day need to make decisions using totally inadequate evidence, are prone to jump to conclusions when presented with very thin chains of inferred relationships. For example, merely plastering a man's name on billboards will markedly change the outcome of an election, if the other candidate's name is not equally displayed.

The use of private detectives to unearth defaming information on political candidates and their associates has become an increasingly prevalent feature of elections and is expected to increase in the future.

The cost per unit of dirt mined by unautomated human garbage collectors can be cut by orders of magnitude once they obtain access to a set of wide-access information systems now being developed. It is the sophisticated form of chain-relation blackmail that may be of the most social concern. The development of geographically widespread access systems uses communications lines to connect the users into the computer. There is a widespread belief—but perhaps not by this committee—that somehow the communications network used will possess a God-given privacy, but "it ain't necessarily so * * *"

THE IMPACT OF COMMUNICATIONS UPON COMPUTERS

Using telephone lines modified to handle digital data, we are able to build an increasing number of geographically distributed time-shared computer systems. Many individual users are connected to a common computer base. Examples of such systems include airline reservation and credit checking systems for civilians and fancy display "command and control" systems for the military.

Simple recordkeeping, a mark of a highly developed economy, has been a prime area of development of these large computer file/communications systems. The development passes through several stages. First, much of the routine clerical work is transferred to a single large computer with few humans nearby allowed to interrogate the system. As time moves on, the number of people who are allowed to directly interrogate the system increases. Next, the geographical distance between the users and the machine increases. And eventually sepa-

rate systems are tied together to improve efficiency. The communication network forms one weak point in the system from the standpoint of eavesdropping and tampering.

Now, for some directions toward a solution.

Assume that not everyone is as honest and as trustworthy as ourselves—but is just as diabolically clever.

Appreciate that we will be dealing increasingly with complex and, hence, difficult-to-understand-all-the-details types of systems in the future.

The people who best understand the operation of each system will be computer designers who build the system in the first place.

The best time for applying fundamental safeguards is during initial system design. "Patchups" at a later date may be relatively less effective compared to good initial design that includes an awareness of the existence and importance of the problem.

We cannot expect and should not expect legislative action alone to substitute for good design. Even ignoring the lag of the legislative/judicial procedure, the detailed subject matter verges on or beyond the limits of legislative effectiveness.

As you know, laws and laws alone have been pathetically ineffectual in stopping the growth of widespread electronic eavesdropping and wiretapping. At most, the courts have succeeded in preventing police from using the same techniques available to the private detective or the criminal—or even a casual reader of an electronics technician's magazine.

While laws in themselves may not solve the problem, new legislation could be helpful in two ways: (a) laws outlawing certain practices will be of minor help in increasing the price of the act and making its commission less flagrant; (b) laws can be written so that potentially weak systems cannot be built unless adequate safeguards are incorporated throughout for the protection of the information stored.

This last direction is to me viscerally unsatisfying as it carries with it a built-in loss of freedom. The creation of another governmental agency peering over one's shoulder contains the possible dangers of bureaucratic delay and arbitrary conclusions based upon inadequate understanding of complex problems.

Historically, Government regulatory agencies start as highly effective bodies but lose momentum as the original personnel leave and their replacements come from the industry being regulated. Where else are you going to get competent people who know the business? The competence needed in a regulatory agency of this type is a too rare commodity.

If the computer industry is to avoid external regulation, then it behooves everyone who is involved with time-shared systems handling potentially sensitive information to start working, or a least thinking, about the problem of privacy. The computer industry should take the initiative and the responsibility of building in the needed safeguards itself before "Big Brother" is forced to do it himself and we may not be too happy with the way he might want to do it.

Safeguards, whether they be screens around moving machinery or circuit breakers, cost money. Every design engineer is reluctant to add anything that costs money and buys little visible protection. But it is time to start regarding such added costs as necessary costs—a price

to society for the privilege of building a potentially dangerous system. When you buy a new system of this type, plan to spend extra for safeguards.

This is not a new concept. We have, for example, been practicing this in the design of sewerage systems and in electrical distribution systems for some time. But, historically, it usually has taken an epidemic to build a local sewerage disposal system. It took a series of disastrous fires to get our electrical codes and possibly the recent Northeast blackout to start work on a better power grid.

The national geographical extent of the new data systems, their impact, and the investment are so large that the price of the "retrofit" after calamities occur may be higher than we need pay with preplanning.

To be more specific, what safeguards do I envision? Of course, we should not know all the answers yet. But, clearly, there are steps that we do not be considering, including:

Provision for minimal cryptographic-type protection to all communications lines that carry potentially embarrassing data—not super-duper unbreakable cryptography, just some minimal, reversible, logical operations upon the data stream to make the eavesdropper's job so difficult that it isn't worth his time. The future holds the promise of such low-cost computer logic, so this may not be as expensive as it sounds.

Never store file data in the complete "clear." Perform some simple—but key controllable—operation on the data so that a simple access to storage will not dump stored data out into the clear.

Make random external audits of file operating programs a standard practice to insure that no programmer has intentionally or inadvertently slipped in a "secret door" to permit a remote point access information to which he is not entitled by sending in a "password."

When the day comes when individual file systems are interconnected on a widespread basis, let us have studied the problem sufficiently so that we can create sensible, precise ground rules on cross-system interrogation access.

Provide mechanisms to detect abnormal informational requests. That is, if a particular file is receiving an excessive number of inquiries or there is an unusual number of cross-file inquiries coming from one source, flag the request to a human operator.

Build in provisions to verify and record the source of requests for information interrogations.

Audit information requests and inform authorities of suspected misuse of the system.

This list is open-ended, and it is hoped that more suggestions will be forthcoming. But this will take much work.

Clearly here is an example of the trade-off between dollars and the type of society we want. We will face such decisions more and more often in the future.

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

If we default on exercising this opportunity and ignore the existence of such potential problems, the word "people" could become less a description of individual human beings living in an open society and more a mere collective noun.

It may seem a paradox, but an open society dictates a right to privacy among its members. Being aware of the potential problems is the first step in preserving this right. I sincerely thank the subcommittee for its efforts in this direction.

Mr. GALLAGHER. Thank you very much, Mr. Baran, for a very profound analysis of the problem as well as something that leaves us sitting here with our mouths open, as we consider in the light of the new technology we possess that "Big Brother" seems to be an infant in the year 1966 rather than 1984 if the technology we now possess were used for that purpose.

Mr. Baran, would you care to comment—I think you were here yesterday for part of the testimony of some of the proponents of the statistical data bank—would you care to comment on the feasibility of a system that could be designed for statistical data collection vis-à-vis an intelligence gathering system? Are they inseparable?

Mr. BARAN. The line dividing the two is an extremely fuzzy one. I think if one wanted to extract intelligence information from a statistical system he could. I could think of one example where a computer society conducted a survey—it has done this a few times—among its members, asking for information about salary, location, fringe benefits, length of service, and number of people employed. This information was sent to a very respectable accounting firm, magnetic tapes were prepared, and we were able to call up information of any type, saying on the average how much does a person make if he has been employed x years, with the following degrees? It soon became clear that we had to be very careful in protecting this tape because we could phrase our questions so that we could pick out people, even though there were no people's names on the tape. Yet the system described yesterday would have people's names and would have social security tags on them. This is a difficult problem.

On the other hand, the protection mechanism suggested yesterday that if the output of the inquiry covers such a small sample, that information is discernible as to precisely who is being examined, then the output is stopped, was also mentioned. This is the sort of safeguard I think one will have to see as a minimum. In other words, I believe the people yesterday were aware of some of the problems. It is unfortunate, I think, that they came in with a preliminary study and had not done all their homework on the safety part of the question. In specific answer to your question, you can extract intelligence information from a statistical system and get statistics from an intelligence system. It is just a little bit easier to use the machine for one purpose than the other.

Mr. HORTON. With regard to this so-called intelligence and statistical system difference, is it possible technically to design a system so that only statistical information could be utilized or be furnished and thus protect the so-called individual information?

Mr. BARAN. If you say I know all the questions I want to ask in the future, perhaps. But if you don't, that means you have to keep the information in raw form. This is the most efficient way of keeping it.

Mr. HORTON. I am assuming you are an expert in this field, the field of computers and what they can do. I am asking you from a technical standpoint whether or not it is possible—in other words, could we pass a law that would require—the construction of a computer that would only produce statistical information that would be foolproof insofar as individual information was concerned?

Mr. BARAN. "Foolproof" is a rough word. I think we could build safeguards to make it difficult. How effective they are, I think, requires a level of detail that we have not examined yet.

Mr. HORTON. The point I am trying to make is that I think any law Congress would enact to safeguard the right of individuals in this area would depend to a large measure upon the state of the art.

Mr. BARAN. That is right.

Mr. HORTON. With regard to the technical aspects, I do not think we have sufficient information to protect the private individual in the computerized systems.

Mr. BARAN. That is right. The technical art is changing very rapidly in computers. The speed of the computer is going up tremendously. The cost is coming down. The size of the memories is expanding very rapidly. As we look to the future we could probably see increases of size of computers—perhaps on the order of 10,000 times as powerful as today's computers.

Mr. HORTON. As a very simple case, if it were possible to pass a law that no computer system could have key A and that key A would be the key that would release personal information, there would be a safeguard. But short of that it seems to me we have a very difficult problem of enacting a law that is going to provide the type of safeguard that we are looking for.

Mr. BARAN. That is right. It is a very difficult problem to solve by law and law alone, because it is so difficult to implement the intent of the law.

Mr. HORTON. Have you given any thought to the technical aspect of how you could build in safeguards to protect private individuals' information?

Mr. BARAN. I think this is going to have to be done on a per system by per system basis. I do not think there is a general panacea. If a centralized statistical information bank is proposed, one would have to look at that particular system configuration very carefully in detail—in nuts and bolts detail—before making any statements.

Mr. HORTON. He could not pass a law for each system or each individual computer.

Mr. BARAN. That is the problem.

Mr. HORTON. How would we devise a law that would cover all computers? This is the problem.

Mr. BARAN. That is right. This is why it is too difficult a problem. All we could do in the way of law is to make misusing the information a crime. We would not expect this to be effective in itself—just increasing the price to those who would misuse the information. But there is no guarantee at all that this would solve the problem.

Mr. HORTON. I was not thinking so much of a crime as I was just to put in adequate safeguards that would prevent the misuse of information.

Mr. BARAN. It is a very difficult thing to do, because we are getting better and better information retrieval techniques. Even if you left the person's social security number off and left the name off, you could probably work backward and pose the question in a certain way and come up with the information.

Mr. HORTON. Were you impressed with the distinction that Dr. Dunn gave us yesterday regarding the intelligence system and the statistical system?

Mr. BARAN. I thought it was an excellent way to characterize their goals. In other words, what they wanted their system to do. Now comes the hard part—how do you build the system that will do what he says and not have the weaknesses that we are all aware of? I think the name of the game is really, how do we build safeguards into the system? We know it is just a matter of time until we get these systems. Clearly what was discussed yesterday was a very preliminary study. I think a lot more homework has to be done and a better definition of the precise safeguards reached. At that time I think we will be able to come up with more precise answers.

Mr. GALLAGHER. Mr. Baran, on the basis of that statement do you feel then that because it was so basically preliminary that it would be premature to attempt to build such a system at this point?

Mr. BARAN. I think the burden of proof ought to be put on the system proposal to show that no weaknesses such as you raised yesterday exist.

Mr. GALLAGHER. Has such a system been devised up to this moment?

Mr. BARAN. The military probably come closest to this. They have very sensitive information and have to transmit it from point to point. They go to a great deal of trouble and expense in keeping their information under control.

Mr. GALLAGHER. Isn't the control there basically one of cryptography?

Mr. BARAN. They have cryptography. They have certain clearances for the people who use the information. They have a system of need to know that is very rigid. And the penalties for abuse of the system are very high.

Mr. GALLAGHER. Is there a system now that can protect from a hardware security standpoint other than cryptography?

Mr. BARAN. I do not know how to answer that one. There are several weak spots in the overall system. You ask, "Can we do the job with other than cryptography?" Cryptography can be done on a software basis as well as hardware. In other words, the computer can generate its own cryptographic key. You would still have to watch your programers and anyone having access to the information.

Mr. GALLAGHER. It basically is radiation transmissional interception.

Mr. BARAN. I think you have to assume that the other fellow will have access to the telephone lines. The information coming out of the computer has to be in such a form that he cannot decipher it. All we can do, I should say, is that we can make the price for breaking the information so high that it is not worth his while. It would never be foolproof. All we can do is raise the price to an eavesdropper to such a point to where he throws his hands up into the air and says, "The heck with it."

Mr. GALLAGHER. This automatically raises the cost of the system itself.

Mr. BARAN. Yes, sir.

Mr. GALLAGHER. Well, beyond the very simple figures that we have been talking about.

Mr. BARAN. I do not know how much.

Mr. GALLAGHER. I think part of the report was that they thought that they could start a system in the area of \$2 million. Is that even conceivable?

Mr. BARAN. I do not know. I have not seen their precise proposal.

Mr. GALLAGHER. Do you think the art is at such a state now that we ought to jump into this type of thing without having thoroughly thought it out?

Mr. BARAN. Heck, no.

Mr. GALLAGHER. We are in agreement with that statement for the very reason you have so ably pointed out. Are you suggesting incidentally to the line of questioning we are on now a possible need for the Federal Government to regulate the intercommunication of informational systems through the interstate commerce clause?

Mr. BARAN. I do not know. This depends on what the computer community does itself. In other words, here we are dealing with a new problem. It has descended upon us. We were not aware of it. All of a sudden we see these individual systems being built. If the computer community is able to understand what is happening and devise safeguards of its own, there may not be any need for the Federal Government coming in. This would be the most desirable course of action. If, on the other hand, we see systems being built without protection, and there is no interest by the computer manufacturers, then it may be necessary for the Government to step into this area.

Mr. GALLAGHER. On the question at hand of a statistical data center, what would you as a private citizen find desirable, or what would you expect the Government to do before we embark on such a course, before you would feel fully secure?

Mr. BARAN. I would just like the assurance that this information would not be misused. And by "misused" I mean passed over to others who do not have a legitimate need for the information.

Mr. GALLAGHER. Do you think there exists now a capability to give you this protection?

Mr. BARAN. I do not know. It is a very poorly studied problem. I speak to you with great ignorance today.

Mr. GALLAGHER. If you speak with ignorance think of the position we are in.

Mr. BARAN. That is right. We are all in the same boat.

Mr. GALLAGHER. Do you think that the people who are suggesting this proposal are beyond this point of ignorance that the rest of us share?

Mr. BARAN. I think we are all pulling on oars in the same boat.

Mr. GALLAGHER. Do you think that they have a broader understanding of computer capacity than you and your fellow experts have?

Mr. BARAN. I have not read their report, but from the remarks of yesterday they had not emphasized their examination of this problem. There is practically nothing to be found in the computer literature on the subject. Hence, I would think that they are not in any better position than the rest of us are in achieving a sense of happiness looking at the efficacy of the safeguards that we would like to see.

Mr. GALLAGHER. Would you agree with the suggestion of this committee that while the results the proponents are seeking are quite desirable, nevertheless the state of the art is at such an early stage that further study of the problem should be had, or there should be a continued study of the problem before we embark on a Federal statistical data system?

Mr. BARAN. I agree wholeheartedly with that statement.

Mr. GALLAGHER. In your statement here, I would like to read this part, where you were "highly pleased" and yet "surprised by the rapidity with which Congress is addressing itself toward the examination of this subject—one that is not yet generally recognized as being a problem by most in the computer profession." Do you think that the computer profession itself should start addressing itself in a more meaningful way to the problem of privacy and safeguards and protection?

Mr. BARAN. I do. I see a small but growing group in the computer profession beginning to become concerned about this range of problems.

Mr. GALLAGHER. Do you feel that before the Government would get committed on a course that we should allow the problem to develop and some ideas generate from the computer profession as to safeguards?

Mr. BARAN. Yes, I think we have the time. The problem we are addressing is a future problem. It is not something where we need an immediate answer today. We could hold off a little. We have the time to think and consider alternative approaches to this question of providing safeguards. Since the details are going to have to be devised by the computer profession, I think it is well that they be encouraged to start working along this direction. They work very well together. We have good industry standards on things like data communication, formats, and coding arrangements, and I am sure that something can be developed along this line in the matter of safeguards.

Mr. GALLAGHER. In view of that statement, that there is time to develop our thinking on this, conversely do you feel that this is not the time to get into a statistical data bank?

Mr. BARAN. If the report concluded that the need for such a center was sufficient, it might be well not to impede what they are trying to do. I think there are things to be done in parallel. I think that study of the data bank could proceed, but I would like to see a fair amount of parallel effort going into the safety aspects of the data bank.

Mr. GALLAGHER. I agree with you that the study should proceed. May I get back to this? Do you feel that it would be premature to embark on the construction of a data bank at this stage?

Mr. BARAN. From what little I have heard about it, I would think it would be premature to start on actual construction, because many of the safeguards are hardware-type safeguards.

Mr. GALLAGHER. Do you know anything about an Air Force research study of how to use computers to call up derogatory information on individuals?

Mr. BARAN. Not as such. I am aware of experimental information retrieval techniques that could allow you to ask questions such as, "What is the relationship between person A and person B?" "Have they ever worked at the same place?" "Have they ever coauthorized a paper?" and draw connections between people or organizations.

Mr. GALLAGHER. Could such a system as that be built in an ancillary way to what we are now discussing?

Mr. BARAN. Yes. Once you have the information you can process it anyway you want to.

Mr. GALLAGHER. You also said that the centralization of the information would result in the loss of an individual's privacy as we know privacy today. Could you explain how privacy could be destroyed by such a system?

Mr. BARAN. Suppose we build our future systems without any safeguards at all and all information—this whole list of records that we accumulate during our life—is available in various systems. Let us suppose these systems are highly interconnected for the sake of economy. Then each and every one of these files can be separately interrogated, asking, "Do you have any information on so and so?" Do you have any information on so and so, and work on back and accumulate all the information you wish. Whether the information is centralized in one central data bank or whether it is spread around the country doesn't make a darn bit of difference. The result is the same.

Mr. GALLAGHER. Basically we could sum up, Mr. Baran, that we certainly should not attempt to impede the growth of technology but at the same time we should start devoting more time to building in safeguards so that this technology can serve man rather than subordinate him to its decisions.

Mr. BARAN. That is right. I do not think we are going to be able to stop technology. I think that decision is not ours. But what we can do is to provide all the safeguards we possibly can. This, I think, is the direction we should be going.

Mr. GALLAGHER. You feel at this moment that we have not utilized our resources in the direction of proper safeguards with regard to the privacy issue.

Mr. BARAN. That is right. As you know, it is a new problem. It is one that we have generally been unaware of in the computer field. It is so new we have just not built a large body of people concerned about this problem. I think the fact that you are holding these hearings will do very much to stimulate interest in seeing that such safeguards are forthcoming. The fact that you are holding these hearings will be sufficient to cause many of my colleagues to go back to the drawing boards tomorrow and start dreaming up ways—better ways—of protecting information.

Mr. GALLAGHER. We want to thank you very much for your contribution here this morning. Mr. Rosenthal.

Mr. ROSENTHAL. Thank you, Mr. Chairman.

In the broadest context, and one I think that perhaps I might understand and some of the American people might understand, it is really quite hard for us nontechnicians to visualize all of the manifestations of the proposal. But putting it in simple context, I seem to fall back on the proposition that it cannot happen here. I wonder if it ever could happen here, if that day came to pass. I think you cited some examples. Perhaps some incident that happened in high school might be fed into a computer. The type of car a person bought, whether he bought a motor scooter which apparently is popular with some people today. What book club he belonged to. What magazines he subscribed to.

What newspapers he subscribed to. Do you visualize that this type of information might some day be used by a less democratic government?

Mr. BARAN. This is the danger. This is the long-range danger. This is one way we could end up with a police state if we are not careful.

Mr. ROSENTHAL. I am not only worried about this being used as the mechanism to get to the police state. I worried about what would happen if the police state or anything resembling it came about because of any political changes in attitude by our people. Then this machinery would be available for us by administrators of that government.

Mr. BARAN. That is right. It would make for an extremely efficient police state if you had such a system.

Mr. ROSENTHAL. Is it the thrust of your testimony today that Congress could not today enact laws to prevent this from happening simply because neither we nor the scientists understand the technology sufficiently to protect society from these machines.

Mr. BARAN. Yes, but with some reservations. I think it is not quite that bad. I think we have some safeguards.

I think there are things that we can do. It is not a binary decision, that unless we do this immediately we are automatically going to end up with a police state. It is a shades-of-gray problem. In general, I tend to agree with your remark.

Mr. ROSENTHAL. I am not really making a remark. I am really inquiring because I find this different for a layman to understand. Is it your position that the technicians should be addressing themselves to the safety-valve features of the machine as much as the scientific development of the machine itself?

Mr. BARAN. Yes.

Mr. ROSENTHAL. And the scientific community has presumably not yet done that.

Mr. BARAN. It is just beginning. That is right.

Mr. ROSENTHAL. Is it because the scientific community is less obsessed than perhaps the Congress is with constitutional rights?

Mr. BARAN. I think there may be a matter of economics. If you could sell a computer system without safeguards and you add safeguards your price is going to be higher than your competitors. There is no economic reason why a computer manufacturer should develop these safeguards.

Mr. ROSENTHAL. In other words, you think we might be the victims of the economics of the situation.

Mr. BARAN. We could be. I think one of the outputs of this committee is making this range of problems more widely known, so that the people who buy computer systems become more sophisticated and ask for the safeguards. So when the bids come in from different computer manufacturers, the increased price will show up in all the bids and there would no longer be a differential factor.

Mr. ROSENTHAL. When you said the committee had an output, you are now taking us into the scientific computer.

Mr. BARAN. Yes.

Mr. ROSENTHAL. On page 17 of your statement, item No. 4, you made the statement, "We cannot expect and should not expect legislative action alone to substitute for good design." That merely supports what you just said informally.

Mr. BARAN. Yes.

Mr. ROSENTHAL. That the scientific community must address themselves by way of design to considering the problems that the subcommittee is considering, to wit, the invasion of privacy.

Mr. BARAN. That is right. Since this is occurring in both the private and public sector and is so widespread, I doubt whether you could sit down and write some laws and pass them that would solve the problem.

Mr. ROSENTHAL. Simply because the technology is not sufficiently advanced for those laws to be written today.

Mr. BARAN. That is right. That is one of the key elements.

Mr. ROSENTHAL. Thank you, Mr. Chairman.

Mr. GALLAGHER. Thank you, Mr. Rosenthal. You said we are in shades of gray. Would not a statistical data bank wash out the gray and replace it with black if we were to adopt it at this stage of the game?

We are talking now as a mechanism of totalitarianism or the police state that you mentioned.

Mr. BARAN. If we are to adopt it without protection possibly.

From the way the gentleman spoke yesterday, at least later in the afternoon they were aware of the existence of this problem. I think a suitable system emerging will have much more in the way of protection than the example that you have cited.

Mr. GALLAGHER. This would call for a great deal more study.

Mr. BARAN. A great deal more head scratching and hard detailed work on a specific system.

Mr. GALLAGHER. Thank you very much, Mr. Baran, for your appearance here today and your really outstanding contribution.

The next witness before the subcommittee is Burton E. Squires, Jr., visiting assistant professor of computer science, University of Illinois, Urbana, Ill. We welcome you here this morning.

STATEMENT OF BURTON E. SQUIRES, JR., VISITING ASSISTANT PROFESSOR OF COMPUTER SCIENCE, UNIVERSITY OF ILLINOIS, URBANA, ILL.

Mr. SQUIRES. Thank you, Mr. Chairman.

Mr. GALLAGHER. Will you please proceed? I saw you wince at a few questions.

Mr. ROSENTHAL. I did, too; I was not sure whether you winced because of the question or because of the answer.

Mr. SQUIRES. Mr. Chairman, I would like first to express my appreciation to you and to your committee in inviting me to these hearings. This is a very difficult and complex area, involving intimate knowledge in the fields of governmental and individual rights, psychometry, statistics, and modern technology. The task you have undertaken, to familiarize yourselves with the essentials of these fields, is indeed a formidable one. Through these hearings you have already made significant progress in protecting our right of privacy. You are now collecting data that will help all of us more reasonably to assess the full political implications of automatic data processing equipment. As you know, my specialty is in the field of computer science, and I will try to confine my remarks to this area. However, I feel quite deeply that we are here dealing with a technology that is as potentially dangerous and powerful as a nuclear explosive device.

It might be helpful to draw some analogy between the present technology in this area and the nuclear-device problem, but I fear the analogy may break down before it proves very useful. There is a very important difference in these problems. The nuclear device threatens to physically destroy our cities and perhaps our country in a rapid series of large easily recognized explosions. The invasion of the privacy of our citizens threatens to carry out a destructive mental process on a gradual, less perceptible scale, under the guise of causes that individually seem justified.

In preparing for this hearing I felt it appropriate to read again John Stuart Mill's essay, "On Liberty," in which he says:

The sole end for which mankind are warranted, individually or collectively, in interfering with the liberty of action of any of their number, is self-protection. That the only purpose for which power can be exercised over any member of a civilized community, against his will, is to prevent harm to others. His own good, either physical or moral, is not a sufficient warrant. He cannot rightfully be compelled to do or forbear because it will be better for him to do so, because it will make him happier, because, in the opinion of others, to do so would be wise or even right. * * * Over himself, over his own body and mind, the individual is sovereign.

This committee has already heard extensive testimony regarding the collection of data concerning a person's thoughts, beliefs, emotions, and sensations. Professor Beaney and Mr. Speiser have testified—on pages 15 and 27, first session hearings—how such data can restrict the exploration of ideas, diminish intellectual curiosity, and restrain the free expression of thought. Mr. Mill's essay also develops these areas more fully. I would like, therefore, to extend these concepts as they relate to automatic data processing.

I cannot stress too much how important it is that this committee and our fellow citizens realize that a computer must be regarded as an information handling device rather than merely an arithmetic device. Perhaps the word "computer" should no longer be used, but rather some other expression such as automatic data processor, or information processor, or, as Dr. Peter Naur has recently proposed, datamation.

In addition to arithmetic operations, a computer can handle alphabetic and linguistic information. It can read, process, analyze, sort, store, and print such information at a phenomenal rate. A high speed computer memory now under development can read and write electronically at the rate of 16 million characters per second. A typical 300-page book contains about 1 million characters. The information storage capabilities are fantastic, although such a fast memory is extravagant in its use of space. It stores only 500 characters per cubic inch and it must be located within a very few feet of the central processor or "main frame" of the computer. Thin films and magnetic tapes are normally used for high capacity memories. A piece of magnetic tape about 0.0015-inch thick and 1-inch square, attached to a computer, can hold up to 3,200 alphabetic characters that can be read at rates exceeding 100,000 characters per second. This media packs information at a density of about 1½ million characters per cubic inch. Thus a building, containing 10,000 square feet of storage space 10 feet high, could conceivably store a book of information about every man, woman, and child in the United States. Specific information about any particular person could be transmitted along any given telephone line within a few minutes.

One often hears the remark that computers can do only what they are told to do. While this may be essentially true, it is practically false. Such a statement completely ignores the speed and complexity of problems that can be handled by a modern digital computer. It is, in a sense, like saying that an automobile won't take you anywhere you can't walk. Now, an automobile is about 15 times faster than walking. A modern computer is about a million times faster than paper and pencil.

However, a computer is a machine, not an animate being. As an automobile performs no better than the skill of its designers and driver, a computer performs no better than the skill of its engineers and programmers. Some of these programmers are extremely skillful and sophisticated. They can write programs which give the computer a kind of "artificial intelligence." In such programs the computer is allowed to operate in a simulated random manner, to evaluate the effects of these random operations, and to modify its own operating program. As a result, the computer can literally write its own programs for the direct solution of a difficult problem. By such means it is sometimes said that computers "learn." After a short time even the programmer has little knowledge of what the machine is actually doing, and he may be unable to predict the future behavior of the machine. The machine is able to learn because it was programmed to do so according to a specific learning theory. In this way the intellect of the programmer is still operating.

Computers now under construction will be able to process pictures as readily as present computers process linguistic information. A whole new era of information handling is upon us. It is quite reasonable to speculate that within the next 10 years computer terminals will be as commonplace as color television sets are today.

There can be little doubt that the establishment of a Federal data center could bring greater economy and efficiency to Government operations. It could do much more. It could make available to the executive branch immediate and up-to-date information summaries on all aspects of our national, business, and personal lives. Whether this can be done without violating the rights of individuals seems difficult at best and unlikely at least.

On the other hand, if the Internal Revenue Service is allowed access to the census data, and if the Federal Bureau of Investigation is allowed access to social security data, and so forth, or if these data are contained on magnetic tape so that they can be easily transmitted from one Government computer installation to another—as they are now or soon will be—then such a data center could come into existence in effect even if not in name.

Because of the rapid advances now being made in computer hardware and programming systems and in methods for handling large data files, the need for concerted activity devoted to the protection of the rights of the individual citizen has become increasingly urgent. The establishment of a Federal data center containing line item information about every man, woman, and child in this country is well within current technology. By line item information, I refer to information such as you might supply in filling out any form or questionnaire: an income tax, census data, an employment application, a security questionnaire, personality tests, etc. This information could be ar-

ranged or used in any manner seen fit by the persons having access to the data.

The motives and momentum of this trend are clear and must not be underestimated or misjudged. They are the good intentions of overly zealous public servants, and their goals are attractive: an honest income tax, instant credit, better employment opportunities due to better files on individual qualifications, more closely controlled production and distribution of consumer goods and thus presumably lower prices and fewer business fluctuations, and perhaps even better mating opportunities for our young people. For the first time we have a machine capable of taking into account and evaluating our individual characteristics, assuming, of course, that these characteristics are accurately known. We may not know how to use a computer for this purpose yet, but clearly it is possible.

We all recognize the necessity for the collection of certain kinds of information, such as credit ratings, for the operation of our complex industrial society. Although we may deplore this secret collection, most credit organizations today disseminate only the barest necessary information. Can we expect the same respect of privacy by a computer?

If the information is in the machine, and if an unscrupulous programmer knows how to get it out, it may be impossible to prevent his access to it. On the other hand, if it is so difficult for a programmer to retrieve the information that it is not worth the bother, the information is secure. How can we guarantee this?

We could, of course, try to avoid this situation in the first place. We could insist that laws be passed to make illegal the collection and disclosure of private records. Although such laws may serve some purposes, and they may significantly delay the effect, I do not believe that laws alone can prevent this information collection and retrieval—any more than laws can prevent automobile accidents. Laws merely specify how individuals ought to behave. They do not enforce that behavior. Our courts punish only individuals caught in the act of illegal behavior. The problem here is that our technological environment may make it difficult or impossible to apprehend certain types of criminals. The evidence of the information contained on a reel of magnetic tape, for example, can be destroyed in a fraction of a second simply by placing it in a strong magnetic field. This can be done as simply as pushing a button, just as today a telephone caller can prevent his call from ever being traced simply by hanging up.

If a felony results from the improper use of an automobile we arrest the driver, not the automobile. Likewise, if a felony results from the improper use of a computer, we must look to the engineer or programmer. Of course, in either case the fault could be due to mechanical or electrical failure of the device. The fault would be easier to detect if the device were designed in such a manner that its operation was unlikely to result in an accidental felony. Conversely, the successful operation of a computer depends upon those who build and maintain it and those who write its programs.

For many years our society has turned only to law for the solution of problems created by our technology. I think it time to expect technology to help solve some of the problems it has created. For some of these problems the basic scientific principles for their solution

already exist. We have already been successful in negotiating a nuclear test ban treaty with the assistance of a device for the detection of nuclear explosions. We must now ask our technology to help solve some of the other problems it has created.

I think the problem of the protection of individual rights in the use of a Federal data center is one of the problems which our engineers and scientists can help solve, at least temporarily.

I am not personally aware of any efforts in this area, but I think it is an area ripe for consideration. By this I mean it is an area in which it would be most profitable for some of our talented physical and social scientists to get together for a serious discussion of the issues and the potential solutions.

Over the years we have asked our talented young people to become scientists and to produce new devices for civilian and military use, and many of our people have contributed significantly in these efforts. We must now ask for the creation of devices that protect our freedom from the misuse of devices already produced. Automatic data processing equipment was not created without public cost and support; even less so will be devices to protect our freedom. Our forefathers did not gain freedom without risking their lives, fortune, and sacred honor. It appears unlikely that we can retain it without similar risk.

Mr. Chairman, that concludes my prepared statement. I would be happy to answer any questions that I can that you or the committee would like to pursue.

Mr. GALLAGHER. Would you care to comment on the proposal before this committee—that of a central data bank—whether or not we are ready and whether we should embark on such a proposal?

Mr. SQUIRES. Mr. Chairman, I have not seen this proposal, nor am I really aware of its economic and political implications in the sense that it is needed by the Government, so in view of my ignorance in this area, I don't think a comment would be appropriate.

Mr. GALLAGHER. Assuming that it could be helpful and that it is needed, from the standpoint of the technology and the lack of our young scientists—or our scientists, as you have pointed out here—to apply their talents to the problem of privacy and safeguards, would it be technologically advisable to embark on this course at this time?

Mr. SQUIRES. From the standpoint of the technology, as I see it, I do not believe we could embark on such a project without knowingly placing ourselves in very grave danger of violating the individual rights of our citizens. Whether this project could be undertaken in pieces in such a way that the amount of intrusion was minimal compared with the rewards that would be gained from such a system, I don't think I could directly comment.

Mr. GALLAGHER. I think you have summed up a problem that is in the area of our concern: that while we have made great advances in technology, there is an imbalance in regard to safeguards set up to protect the individual, his privacy, and his future sufficiently, in light of the advance of technology.

You state here:

However, I feel deeply that we are dealing with a technology that is as potentially dangerous and powerful as a nuclear, explosive device.

Would you care to elaborate on that sentence?

Mr. SQUIRES. One way this country could be turned into a police state is by means of a military force, conceivably. We go to great expense and effort to prevent this from happening. Our activities in southeast Asia are indicative of the cost which this community is willing to endure in an effort to prevent any such occurrence.

Mr. Baran has testified already this morning how the information contained in such a system could be used to create a very efficient police state. One might even say that, similar to the way coups occur in other countries, one would capture the building in which all this information is contained and one might be able to establish a police state just by virtue of having the information in his hand.

Mr. ROSENTHAL. Instead of the radio station, they capture the machine.

Mr. SQUIRES. You capture the information center because the information center is not only going to contain all the information you need to know to run the state, but very likely in the future it may contain all the information you need to control the flow of information.

Mr. GALLAGHER. And you agree substantially that a statistical data center could easily become a center of intelligence on individuals?

Mr. SQUIRES. Yes, it would be.

Mr. GALLAGHER. Do you see any way presently, in view of your experience, that the two could be separated?

Mr. SQUIRES. It would be most difficult. I would not say it would be impossible.

If the way in which you stored the information—this was alluded to by Mr. Baran—were not in raw data form, that is to say, if the way in which the information was stored was in the form of statistical summaries in which no summary dealt with fewer than say 100 or 200 people or some arbitrary number that would be sufficiently high to guarantee individual privacy, then of course at no time could you retrieve any such information out of the center because it wouldn't be in there. It was there only while it was being collected, and it was immediately destroyed.

On the other hand, this makes it difficult or almost impossible to ask at some later time a question which you had not previously anticipated asking at the time you made the summaries. Consequently, the information you collected is not nearly as useful as it might be because you have no ability to reorganize it in a different way simply because you destroyed it after you collected it.

Mr. GALLAGHER. Mr. Squires, on the question of liberty, where you quote John Mill's essay, you went on and your whole presentation gave the illusion that liberty could be fast disappearing in the new environment upon which we are now entering.

How can liberty be protected if these things will happen anyhow? Assuming somebody could get into the computer center?

Mr. SQUIRES. That is a very difficult and disturbing question, Mr. Chairman, and it is one which disturbs me and I frankly do not know the answer. I do feel that we ought to address ourselves to this question in a very real way in our society. I do feel it is a question to which we can address ourselves intelligently, but I don't necessarily feel that it is a question where we will be able to come up with answers without a great deal of effort.

Mr. GALLAGHER. What would be your suggestion to at least get on a track headed toward this end?

Mr. SQUIRES. My immediate suggestion would be to sponsor some sort of symposium in which prominent people and talented scientists and social scientists were invited to present papers on this subject and in which a reasonably small number of these people could get together and sit down and think up a lot of ideas.

Mr. GALLAGHER. You think this should be sponsored by the government, or some of the foundations or combinations of both? How can we get those people most qualified to think about this problem, to crank up and start doing something about it?

Mr. SQUIRES. Again the fact that you are holding these hearings I am sure is going to gather a good deal of attention among some of the foundations and perhaps just by virtue of what comes out of this hearing some of them might be willing to sponsor such a symposium. I do not know.

Mr. GALLAGHER. You, however, feel that it is a critical problem in the light of your testimony that we do start gearing our thinking in that direction?

Mr. SQUIRES. Yes, Mr. Chairman, I do. Personally I doubt that the computer community can be expected to come up with these safeguards on its own initiative without some help from foundations or from the Government or both, or some other sources.

Mr. GALLAGHER. Should this not be a joint effort with the social scientists? Some of the social scientists, by the way, are those who are strongly urging this statistical data center. I think there is a general unawareness in the community of the problem. Not an unawareness, perhaps just a lack of attention to the central problem that we are discussing here this morning.

Mr. SQUIRES. I am suggesting partly that it be a joint effort in that as a computer professional I'm really unable to evaluate the problems that the social scientist has. In a discussion between computer professionals and some social scientists, we might be able to come to some understanding as to what kinds of information the social scientists have to put in the machine, and what kinds of information they have to get out. Once we have this understood, the technology is in a much better state of being able to understand how to build some hardware that would have these protections in it.

Some of these protections can be built with software; that is, by programming efforts, but it seems to me basically it has to be built into the hardware, as Mr. Baran is also suggesting. I don't see how it can be built into the hardware unless the people building the hardware are aware of the kinds of safeguards that are really required. This is the reason I suggested a joint effort at this stage as appropriate.

Mr. HORTON. It seems to me also, Mr. Squires, at this point that it is well to differentiate between the control or the regulation in the public aspect—that is, through the Federal Government and governmental activity, and also in the field of the nongovernment.

As I understood the testimony, this is not a problem which could come about 5 or 10 years from now, but it is a problem that faces us right this very minute. We have before us just this one proposal with regard to a centralized data center, or a data bank. But there already is widespread use of this both in Government and outside of Government. So it would seem to me that these considerations of the protection of privacy, from my standpoint anyway, have a Federal interest, even though some of these computer systems are nongovernment.

Now, would you tend to agree with that aspect of it?

Mr. SQUIRES. Yes, I would.

Mr. HORTON. That we think in terms of protection of the individual's rights in the nongovernment aspect of our society in addition to the governmental aspect of our society.

Mr. SQUIRES. Yes, I definitely think so.

Mr. HORTON. I would like to ask you this: Are you in the technical aspect of computers? In other words, what is your specific field?

Mr. SQUIRES. Well, specifically I am working on programing systems.

Mr. HORTON. Are you an expert in the technology of computers, or are you more an expert in the field of the philosophy, or the use of computers, or both, or something else?

Mr. SQUIRES. I am afraid I don't really know how to answer that question.

Mr. HORTON. Do you design computers?

Mr. SQUIRES. No, sir, I do not design computers. I am presently at the University of Illinois. There are fellow scientists with whom I work who do design computers. My activities are more along the programing line, designing the programing systems, or software, as we referred to them in the testimony.

Mr. GALLAGHER. In other words, you engage in the computer sciences?

Mr. SQUIRES. That is right.

Mr. HORTON. You are more in the programing or use of computers as opposed to how they are built and designed, is that right?

Mr. SQUIRES. Yes, sir.

Mr. HORTON. Then I think this question is properly in your area: Do you have any suggestion as to how, programwise, this committee can make any recommendations or take any action which will protect the individual's rights in the use of the computers?

Mr. SQUIRES. I think some things can be done programwise, but they are somewhat minimal in that the information is stored in the machine somewhere.

One way of getting this information out of a computer is to do what is called a dump; what this amounts to is connecting the tape or whatever the storage device is to the computer and asking the computer to print out just exactly what is on this storage device. You then get a hard copy record of what was there. What you are asking is, is there a way to prevent a program from doing this? Strictly from a programing point of view, I do not believe there is.

Now, the information could be stored in the machine in cryptographic forms or it could be sorted and this should be done, as Mr. Baran has suggested, but even if it is in a cryptographic form, if a person knows the code or can invent a decipher for it and he has access to the computer, he can write a program to decode it. So I don't see programing alone as being the solution. I think it will have to be partly programing but a large part of it will have to be associated with the hardware.

Mr. HORTON. In other words, to define the areas with which we have to be concerned, we must consider how safeguards can be built into the technical system, that is, the mechanical system of the computers, and the whole problem of telecommunications and its ac-

cumulation and output of information. Then it also seems to me that we have to be concerned with building safeguards into the programs that are going to be involved in the use of the computers. Likewise, I feel we have to be concerned about the application of the system and the programs in the Federal Government or outside the Federal Government and build in safeguards in those areas.

Now, it seems to me that we haven't had very much information in any one of these areas until this subcommittee became interested in it, but I think you have indicated, Mr. Packard and others have indicated who have testified before us, that it is a very complex problem and that there isn't any safeguard at the present time in any one of these areas that will protect this interest that we are concerned about.

Mr. SQUIRES. There is some activity in the sense that people building time-sharing computers—particularly at MIT, for example—have developed systems whereby presumably a given user may not have access to another user's files. However, there are also other people in the field who claim that there hasn't been built a system that they can't break, so it is pretty primitive at the present time.

Mr. HORTON. In Mr. Macy's article in the Saturday Review of July 23, 1966, he makes reference to an integrated system and how this can be beneficial to the selection of personnel to fill jobs. He indicates some of this system has already been used in presenting candidates or prospective people to fill jobs at the Presidential appointment level. He also talked about direct tape-to-tape feeding of data from one department to another. It points out that this may become common.

I assume from what you have said and from what other witnesses have said that this is a possibility and in all probability is now in existence.

We also heard from the Government witnesses yesterday an indication that they would not furnish this intelligence information to various departments of Government, but I assume from what you and Mr. Baran said that it is possible to set up the system this way and possibly it is already set up this way.

Do you have any suggestion as to how, programwise, the Congress can deal with the restrictions on the use of this type of information from a central body of information to the various agencies?

Mr. SQUIRES. No, I don't, really. I read Mr. Macy's article on the plane, and read the quotation you just made and even made a copy because I was somewhat impressed by it. The idea of these existing channels is to me somewhat frightening. I can appreciate the problems that people running these systems have and I certainly appreciate their concern as a citizen that intelligence data will not be transmitted on these channels.

On the other hand, I do not see any visible means to prevent such transmission should the parties controlling the machines at any level decide to put such transmission into effect.

Mr. HORTON. It is a complex system that has already been built up to a large measure. I guess you would agree with that, would you not?

Mr. SQUIRES. Yes, sir.

Mr. HORTON. And much of this information is probably already available and it is now just a case of getting it in one central Federal system, or one central Federal place. Even though it is going to be proposed for statistical information only, the information will be there. Then the thing that bothers me is not so much that there may be the fellow who can steal the information or can tap in, eavesdrop, pick it up and disseminate it, but that it is going to be the call in 5 or 10 years from now on the basis of, "This is good for the country. This is something we need to know." In this way, these personal rights will be dissipated. This is a concern I have, too. In spite of the benefits of the system and the good that can follow from having this information, tapping it in and taking it for the public good will in essence do away with the individual's rights because all this information can be gathered in one place.

Mr. SQUIRES. I don't think the gathering of it physically in one place is at all a prerequisite for the existence of a Federal data center, or whatever you want to call it. Perhaps it is in terms of this specific proposal, but in more general terms, the physical location of this data in one place is not at all necessary.

Mr. HORTON. But this does create problems because, as I have understood it, the dispersal of this information at the present time is one of the safeguards that we now have. But if it is centered in one place, then it becomes a more serious problem, doesn't it?

Mr. SQUIRES. Yes, I would say it does.

Mr. HORTON. I think what we are concerned about now is the centralization of this, although I think our attention is going to be somewhat directed to the fact that some of this information is already gathered in some of these specific agencies and it is being used.

Mr. SQUIRES. It seems to me that one of the real problems we face as we gather more and more of this data is that it is difficult to make an intelligent and informed judgment on whether the need to know is as urgent as the need to protect the rights of the individual. When one queries general, popular sorts of opinion and points out the social advantages of knowing this information, the popular opinion will tend to say, "Let's have it," and, "What's all the secrecy about" and, "Why does he want to protect this information. Is he some kind of a criminal, or what?"

It will tend to point the guilty finger at those trying to protect our rights of privacy.

Mr. HORTON. I thank you, Mr. Squires. I think you have made an excellent statement and you have outlined to us what the problem is in this whole area. I appreciate your coming before the subcommittee.

Mr. GALLAGHER. Mr. Squires, would you agree with Mr. Baran that any statistical data center, at the stage we are now in the computer business, that it would not be impossible to identify an individual if his records are programed into the data center?

Mr. SQUIRES. This depends not only on how the information is stored perhaps, but also on the kinds of access that are allowed to it. Let me suppose, for example, the information is stored in the system in such a way that there is no identity given. The social security numbers are completely divorced from the rest of an individual's file, for example—

Mr. GALLAGHER. You were not here yesterday. Mr. Dunn and Mr. Ruggles said that in the interests of statistical research it was necessary to have some identification of the individual—his name or his number. With that being part of his file, would there be any way in which he could be fully protected if someone wanted to get to the information as regards his personal characteristics?

Mr. SQUIRES. Fully protected, I would think not. Substantially protected, quite possibly.

Mr. GALLAGHER. Let's say the supreme commander of the control center wanted information. Could he get it if that information is in a statistical data center, as opposed to calling it an intelligence data center?

Mr. SQUIRES. If I understand your question correctly, what you call a statistical data center and what you call an intelligence data center does not differ in terms of the kind of information that is stored therein, is that correct?

Mr. GALLAGHER. Yes, that is the point I am trying to make.

Mr. SQUIRES. And if the information is stored in there and we do not have safeguards to prevent its being disseminated—and it appears to me at the present time we do not—therefore, my answer is clear. It could be gotten out.

Mr. GALLAGHER. Another intriguing question I always find of interest: Since the IRS has now set up a central data collection service and now that we have the potential of erasing from the computer's memory and truly making a person an "unperson," would it be possible for a skilled computer expert to make himself a nontaxpayer, by programing himself out of existence?

Mr. SQUIRES. That is a very interesting question. I suspect that it would be.

Mr. GALLAGHER. Therefore, by sending in the wrong card or the right card, or the wrong answers, he could be eliminated from existence from the rolls of the IRS.

Mr. SQUIRES. That seems to me quite reasonable.

Mr. GALLAGHER. And we have a "Ministry of Truth" where a person could be programed out of existence and become an "unperson."

Mr. SQUIRES. He would no longer be on the tax rolls at least.

Mr. GALLAGHER. Similarly, a person who might conceivably be in a data center and who would not want to have the information there—he too could be snapped out of existence by a proper program if such a program were set up, so there are two sides of this coin: One, a maximum amount of information on an individual and two, a person with the right key—or, as I said yesterday, the janitor who might have a key over there so he could get in to sweep up—he too could become an "unperson" on the rolls of the Government.

Mr. SQUIRES. This is conceivable.

Mr. GALLAGHER. Mr. Squires, I wish we could go on, but time is running. We want to thank you very, very much for your excellent presentation here this morning.

Mr. ROSENTHAL. I am going to pass and refrain from asking any questions in view of the fact that the House is now in session.

I have visions of Charlie Chaplin in "Modern Times," coming in being the janitor, coming in late at night and eliminating himself.

Thank you very much.

Mr. GALLAGHER. We thought it would be useful to hear about an experience of a State setting up a computer system. Mr. Robert Gallati, as director of the New York State Identification and Intelligence System, has volunteered to come before this committee to give us the benefit of his experience with such a system. The Chair would therefore like to call Mr. Gallati.

STATEMENT OF ROBERT R. J. GALLATI, DIRECTOR, NEW YORK STATE IDENTIFICATION AND INTELLIGENCE SYSTEM; ACCOMPANIED BY ELIOT H. LUMBARD, SPECIAL ASSISTANT COUNSEL FOR LAW ENFORCEMENT TO GOVERNOR ROCKEFELLER, AND EDWARD DeFRANCO, EXECUTIVE ASSISTANT TO THE DIRECTOR

Mr. GALLATI. Thank you very much, Mr. Chairman. I would like to say that it is quite a privilege and an honor to be here and to testify before the Special Subcommittee on the Invasion of Privacy of the House Committee on Government Operations.

I believe I might tell you a little bit about the New York State Identification and Intelligence System from the perspective of one who came from and was a member of the New York City Police Department for a little over a quarter of a century.

Mr. GALLAGHER. My father was a member of the Bayonne Police Department.

Mr. GALLATI. I had the position of assistant chief inspector, chief of planning, on the New York City Police Department when I was first invited by Mr. Eliot Lumbard, who sits on my left as counsel today, to participate in an advisory committee meeting to consider the creation of an information-sharing system for the agencies of criminal justice in New York State.

Among those on the Advisory Committee, besides myself and Mr. Lumbard as chairman, are representatives of the New York State Association of Chiefs of Police, the New York State Sheriffs' Association, the New York State Police, the head of the State parole board, representatives from probation, representatives from the New York State District Attorney's Association, and members of the staff of the department of correction, and members of the staff of the judicial conference. Represented are the six major branches or functions, if you will, of the administration of criminal justice. The police, prosecutors, criminal courts, probation, institutional services, and parole. We are joined by members of the Systems Development Corp., a "not for profit" organization engaged in various system development endeavors and at that time—and I believe subsequent thereto—engaged largely in Air Force contracts relative to the SAGE system. We discuss matters relating to the need for information sharing.

As I am sure you are aware, New York State is a large State and has tremendous geographic area, which causes a diversion in a sense, of the various jurisdictions on the horizontal, or geographical area, if you will.

Mr. GALLAGHER. Coming from the other side of the river, I sometimes question the jurisdictional rights, especially the claims to the "offshore islands" of New Jersey.

Mr. GALLATI. We welcome our sister State of New Jersey. As a matter of fact, we had last night the annual conference of the New

York State Chiefs of Police and we had as a guest Chief Harry Knowles who is president of the New Jersey State Chiefs of Police.

Mr. HORTON. You are covered well in the hearing today.

Mr. GALLATI. In the State of New York there are some 70 million files in the various agencies of criminal justice. We are aware of the fact too that in the operation of criminal justice in New York State, as well as elsewhere in this country, the police, the prosecutors, the criminal courts, probation, correction, and parole agencies, deal with the same person through a process, a criminal process, a process of Justice, and the same basic goals are shared by these various agencies for the social good.

In the process, there is a redundancy of investigation. There is also a redundancy of recordkeeping.

And so on the vertical level, if you will, we were made aware in our deliberations of the unitary nature of the process administering criminal justice and, therefore, the compelling conclusion that perhaps a unitary system of compiling and distributing and sharing information would be something to be seriously considered. Information is the raw material of criminal justice action.

The questions that were raised were, of course, what information should be brought together and shared, and we went into a considerable study of these matters and many things were accepted and many things were rejected as appropriate or inappropriate for storage in a central information-sharing system, be it computerized or manual.

It was thought that the tremendous amount of data which would be part of a system of information sharing such as contemplated by the advisory committee, would require the advances available to us in the area of data processing and also, concomitantly, the advances available to us in the fields of communication.

So we developed, with the cooperation of the advisory committee and the consultants from the System Development Corp. a feasibility study which was the beginnings of the creation of the New York State Identification and Intelligence System. That was in 1963, and in 1964 I had the honor of being appointed by Gov. Nelson A. Rockefeller as director of the emerging New York State Identification and Intelligence System, or NYSIIS, as we call it. My appointment was nonpolitical. I was never asked about my political persuasion, nor, indeed, has any member of the NYSIIS team been so asked.

The system was located in Albany, centrally located within the State of New York, and we dedicated ourselves to this concept of cooperative information sharing among criminal justice agencies, within a context of security and a climate of concern for the protection of individual rights and liberties. NYSIIS, therefore, was given no operational responsibilities and when a statute was passed officially creating the agency, it was established in the executive department, responsible directly to the Governor.

The bill which created NYSIIS and which I would like to later submit with your permission, Mr. Chairman, for the record, establishes NYSIIS as an independent agency having no powers, duties, or facilities to arrest, investigate, prosecute, confine, or supervise; no dual obligation, no feeling upon my part as director that perhaps I would be guilty of nonfeasance if some information indicated to me that I should pursue this investigatively.

It was conceived also, as a voluntary system and the participants were free to participate or not to participate, as they pleased, and to determine for themselves the degree of their participation.

Access to the information is to be security controlled, it is confidential and is not available to employers, to defense counsel, private detectives, or anyone other than the user agencies officially engaged in the administration of criminal justice. Nor, of course, would it be available to the mass media. Dissemination of information entrusted to the system is restricted in accordance with the wishes, the will, and the desire of those who contribute the information to NYSIIS.

NYSIIS restricts the input of information to avoid entry into the system and into the data base of wiretap information, such things as grand jury minutes, the identity of criminal informants, and likewise the system will not—

Mr. GALLAGHER. Excuse me, Director Gallati. You say "restricts to the system" or "restricts from the system"?

Mr. GALLATI. To bar from the system the identity of criminal informants, and likewise the system will not accept such information as tax information, social security, unemployment insurance, voting information, or family court data. These exclusions were the result of a long series of meetings of the NYSIIS advisory committee and this committee, as I mentioned before, represented leaders in all branches of criminal justice in the State of New York.

They made careful, considered, value judgments as to the inclusion and exclusion of various types of information which would or would not be included in the NYSIIS data base.

We were very much concerned from the outset about the problems of civil liberties and civil rights and constitutional guarantees. It is very difficult for anyone in the field of criminal justice today to ignore the imperatives of these considerations, particularly in the light of recent decisions of the Supreme Court; one has to be continuously alert to the implications of constitutional guarantees. And, of course, as in the *Miranda* decisions, we were reminded that we need to be more efficient in our criminal justice efforts and that we should utilize the facilities available to us presented through research and development, through science and technology, to do a better job in criminal justice.

Mr. ROSENTHAL. Inspector Gallati, does the statute that set you up limit the people that you can provide information to?

Mr. GALLATI. This sets up the limitation that it is designed for qualified agencies concerned with the administration of criminal justice. And it expressly states that this means courts of record, probation departments, sheriffs' offices, district attorneys' offices, State division of parole, New York City Parole Commission, State department of correction, New York City Department of Correction, and police forces and departments having responsibility for enforcement of the general criminal laws of the State.

Mr. ROSENTHAL. Can you give it to an outside State agency?

Mr. GALLATI. No, not to one who is not a user or who would come under these categories.

Mr. ROSENTHAL. In other words, you don't provide information if the State of New Jersey asks you for something about an alleged criminal, you would not provide the information?

Mr. GALLATI. This is not set up, yet, as an operating system, as I will mention shortly.

Mr. GALLAGHER. But with two friendly chiefs—a friendly chief in New Jersey and a friendly chief in New York—the friendly chief in New Jersey could call his friend in New York and get information that you have?

Mr. ROSENTHAL. In other words, they could short circuit the system.

Mr. GALLATI. Well, this is not now an operating system, Mr. Chairman, and the situation which you propose is one which we are considering in terms of our total development. We feel, in reference to this matter, that the improper utilization of the information in this system by any user would be one of those things which we would concern ourselves with greatly in terms of overall security and also in terms of the internal discipline of the users within the system. So that today, when sharing of information might conceivably be improper between two chiefs of police, a lesser penalty would derive therefrom in the eyes of the chief from breaching any confidentiality than would obtain in a system of this type where he would be cut off from sources of information because of his failure to comply with security directives.

Mr. GALLAGHER. Yes, but there might be a criminal in New Jersey that you have in your files and they are trying to cooperate with each other.

Mr. GALLATI. Well, today, of course—

Mr. GALLAGHER. In order to bring him to justice.

Mr. GALLATI. There is a series of cooperative endeavors among chiefs of police and people in the agencies of criminal justice which is on a voluntary cooperative basis between chief to chief, agency head to agency head, and it is this that we are trying to encourage in our own State so that we can maximize the information sharing which exists.

Mr. GALLAGHER. Therefore, this information could really be transferred to another State quite easily on an unofficial basis?

Mr. GALLATI. This information could not be transferred in the sense of the data base transferred to another State, except through interface techniques which would be possible if, for example, the State of New Jersey were to develop a system similar to this and we then considered the problems of interface.

Mr. GALLAGHER. No. What I am saying is you have a chief who is a user of your information in New York, properly authorized. Now, he acquires information and he gets a telephone call from somebody in New Jersey saying, "What do you have on John Jones?"

Mr. GALLATI. Well, of course, the user of the system will receive from the system that information which he has a need to know, a right to know, and which the contributor of the information has said this person can receive. Corruption, of course, is always possible; however, it will be extremely difficult and it will be heavily prosecuted and punished. I would like to remind the chairman that we did mention the fact that the person who contributes the information can put whatever restraints he desires upon the information which we then would be required to respect. In other words, if he were to say "I will put this information into the system but only my own agency can retrieve this" or "only my own agency plus this agency and that agency and that agency," we respect this type of constraint, and necessarily so.

Mr. ROSENTHAL. Does your computer have the technical ability to accept the information with restraint?

Mr. GALLATI. Yes. We are so advised by our computer experts, and I might state at this time that we have a man from System Development Corp. who is both a computer expert and an expert in the field of security, assigned full time to advising us on how we can develop the system along these lines.

Mr. ROSENTHAL. The answer to my question is yes?

Mr. GALLATI. Yes.

Mr. HORTON. One other question on this system—

Mr. GALLATI. I think Representative Horton wishes to ask a question.

Mr. HORTON. No; go ahead and answer his question first.

Mr. GALLATI. What I would like to point out is that the system is still in the developmental stage. The system will be operational in terms of building block 1 in August of 1967. Included in building block 1 on August 1967 will be, No. 1, the facsimile transmission system which we are now developing and are beginning to install. We will make primary installations or first installations in the early fall. We now have operating between Rochester and Albany and between Mineola, with the Nassau County police, and Albany, a testing device whereby we are able, through facsimile transmission of fingerprints, to transmit a set of prints from Rochester or Mineola to Albany within 14 minutes; a hard copy is received in Albany. It is there searched through our regular searching procedures and is returned—the criminal history response is returned again by facsimile within 4 minutes to Mineola or Rochester.

I would like to say—

Mr. HORTON. I would like to ask one question.

Mr. GALLATI. Surely.

Mr. HORTON. We have a quorum call and we are going to have to go over and answer the quorum. But are there any criminal restrictions on the users of this information concerning their dissemination of the information or is this wide open?

Mr. GALLATI. The general laws of the criminal code and the criminal law place restraints, of course, general restraints, upon the misuse of information, misfeasance of public officials and, of course, the failure of public officials to perform their duties in the sense of nonfeasance, as well. The general criminal law—

Mr. HORTON. In other words existing laws are considered to be adequate to cover the user's dissemination of this type of information?

Mr. GALLATI. As far as we now can anticipate, the answer would be "Yes," Congressman.

I point out, too, that we would also have the laws of bribery, corruption, laws aimed at corruption, and so on, which would be part of the total picture in terms of the discipline of the system from the user's standpoint.

Mr. GALLAGHER. Director Gallati, while I am thinking of it, you used the figure of 70 million. That is about one criminal for less than every third American.

Mr. GALLATI. Well, I think, if I may suggest this is more in terms, of the mass of data which is acquired by the number of autonomous agencies, independent agencies that are involved frequently with a limited number of persons. The point being, of course, that it does illustrate the duplication of files.

Mr. GALLAGHER. I see.

Mr. GALLATI. Many of these files are resting in one police department, also on the same person a file would be resting in another police department, and, likewise, as you go through the process of the criminal justice agencies, more files become built up as we go along. These files are being searched at the rate of 8 million files per year and they are being searched at great expense to the local communities.

Mr. GALLAGHER. Does a citizen have an opportunity to check to see if his name is in your file?

Mr. GALLATI. No.

Mr. GALLAGHER. As far as its accuracy is concerned?

Mr. GALLATI. No. We have no provision for that, Mr. Chairman.

Mr. GALLAGHER. Supposing Governor Rockefeller wanted to appoint somebody to a job, and a routine police check was made to see whether or not he has a police record, and your computer threw up the fact that there was a flag on him. Who determines the accuracy, or is it institutionalized for life that he might have taken a ride on the wrong bicycle at age 16?

Mr. GALLATI. The files, like criminal files generally, of course, are confidential. There would be in this particular instance you cite, where a public official would be investigated either by the Civil Service Commission, or, in the case of an appointed official, by the State police, they would utilize our files just precisely, in effect, as they now utilize the central identification files. Then it would be up to the appointing person or the appointing agency or the Civil Service Commission, as the case may be, to be guided by whatever rules they may have in terms of disclosure. Certainly, if any time that we are made aware of any data in the bank which might be in any way inaccurate, we would make every effort to remove it. I think that our files, potentially, would be considerably more accurate than those files which might be kept in local agencies where there would be less resources to keep them accurate and perhaps less resources to make sure that they are secure.

Mr. GALLAGHER. No. What I am saying is if a person is not on notice as to what is in his files, how would accuracy be checked?

Mr. GALLATI. Well, I would assume that when he has occasion to be accused of something or to—

Mr. GALLAGHER. He never is, he is just sort of a law-abiding citizen now, sufficient for the Governor or somebody to appoint to public office. It would now be very easy to ask for a profile on him from your computer. He doesn't know what is in there, but it is institutionalized—a rumor or a letter or whatever it might be that would cast an aspersion on his character. Therefore, the computer would throw out or not throw out his name as a bona fide risk.

Mr. GALLATI. Well, this would be something which would be within the purview of the executive chamber. We would respond with the type of information that we will have in the file, to the agency or the person or the official who makes the proper request. Our dealing in this case, of course, would be with the State police, with the Civil Service Commission, or an official user agency. So that we would then, of course, have a dialog between them and ourselves, if there were something that needed to be discussed in connection therewith. The real remedy necessarily lies in the judgment of the appointing authority and how he uses the information he receives—as it is today. NYSIIS

makes no such judgments, and indeed judgments will be made in the future by the same persons, in the same manner, as today.

I would like to point out that while we, of course, are concerned with the negative aspects of the possible violations of civil liberties, civil rights, and constitutional guarantees, that there are a number of very positive effects that this system has.

As a matter of fact, we are very much concerned with the positive effects just as we are with the possible negative implications. For example, we have had a very close relationship with the Vera Foundation and I would like, if I may, at the conclusion of my testimony to submit to you a letter from Mr. Sturz, the director of the Vera Foundation, in which he supports our efforts and recognizes the benefits that can be derived from being privy to, as soon as possible, the fact that a person does or does not have a criminal record which may relate, No. 1, to whether or not he should be bailed; No. 2, whether or not he should be summoned in lieu of arrest; and, thirdly, whether or not he should be released on his own recognizance at the time of judicial determination and also to what extent he should—

Mr. GALLAGHER. This recommendation is in the computer?

Mr. GALLATI. No, Mr. Chairman. May I clarify that, please? The point is that in the Vera Foundation studies on the bail problem and on the summons in lieu of arrest situation they found that it was possible, where a person could not otherwise raise bail, because of being indigent or not willing to take those steps necessary to notify friends, concerning the plight of the person arrested, that an investigation, rapidly conducted by representatives of the Vera Foundation, could determine whether the person had roots in the community, was not dangerous, not a dangerous person to the community, that he could be relied upon to appear for trial. This proved to be most successful and many people were released on their own recognizance on this basis. Likewise, many people, in experiments conducted by the New York Police Planning Bureau in New York City and by the Vera Foundation, it was found that a summons could be issued in lieu of arrest.

So that the indignity of a person spending a night in jail for a minor offense could be avoided, in cases, such as we found in the 14th precinct on 30th Street, where many housewives, people who were perfectly reputable, succumbed to a momentary decision to steal a slip or other item of clothing, and were arrested for shoplifting. These ladies because of their tremendous embarrassment were unwilling to notify their husbands or their parents, but were saved from this indignity of being locked up overnight with people of lesser repute. And, of course, the obvious saving that this ultimately will entail in terms of our unhappy police responsibility of keeping people in the lockup overnight, is quite obvious. But I would like to point out also that the Vera Foundation is now moving into the area of more serious crimes, crimes which are fingerprintable. The utilization of NYSIIS for the rapid transmission of fingerprints in those cases where fingerprints are available, of course, means that many people will not have to be kept in jail overnight, and in the alternative, may be summoned and, in other cases, released on their own recognizance.

Mr. GALLAGHER. Are you tied in with the Federal Bureau of Investigation?

MR. GALLATI. No, we are not. The records in the State of New York have been utilized for these purposes by the Vera Foundation and have been found to be—

MR. GALLAGHER. No. I meant on the transmission of fingerprints.

MR. GALLATI. No, sir, we are not.

I would like to also mention in this connection that the judge has, through this type of system, at his fingertips a great deal more information than he would otherwise be able to assemble quickly in reference to the individual whom he must deal with. And, therefore, he can more discreetly or in discreet fashion sentence in those cases where a conviction results or may release on his own recognizance the person before him, if this is an appropriate decision to make. If the court is uninformed, the court is liable to err on the side of keeping the person in jail.

I would like to continue the point which we made about the process of criminal justice at the point of arraignment, because I think here again we have a situation where, through the utilization of this facsimile system, which is one of the parts of Building Block One of the system, we will be able to overcome some of the very problematic areas of rapid arraignment requirements. I am sure we are all aware of the need for rapid arraignment and the implications that are bound to arise in those cases where arraignment is unduly delayed.

Now, one of the problems that the police have always had has been this problem of making sure what the prisoner represents and, of course, fingerprinting gives us complete, thorough and incontrovertible identification if we have a set of prints for this person on file in the Central Identification Bureau. And also, of course, a record of his criminal history, if such is the case.

Now, the situation in which the police are placed in terms of rapid arraignment is this: When they have a prisoner and they can legally fingerprint the prisoner, they must learn one of two things. They must either assure themselves from the criminal record received, as the result of the submission of the fingerprints, that this person is not wanted for a more serious crime elsewhere, or, is in fact wanted for such a crime and must so advise the judge, upon arraignment, as to the status and the criminal record of the person whom they present to the arraigning magistrate.

The seriousness of this is not to be underestimated. For example, in the city of New York the police department maintains at considerable expense to the city of New York a bureau of identification which is very largely redundant and duplicates the same type of file, although perhaps more extensive, maintained by the State in Albany, but, because of the requirements of the New York City criminal courts and the desire of the New York City Police Department to present what is known as the yellow sheet the criminal history at the time of arraignment before the magistrate, they have maintained in the city of New York at a considerable expense, perhaps in the neighborhood of \$2 million yearly, a duplicate type of facility to enable them to respond in that fashion.

We feel with this new facsimile system and our increased capabilities for the search of our fingerprint files that we will be able to respond in such fashion that rapid arraignment will be possible in New York City based upon those files which we in NYSIIS maintain, but

also similar rapid arraignment will be available to, and discreet arraignment, I might add, available to the chief of police or the detective in any department, regardless of how small, throughout the State.

So, we see we have the potential for civil liberties advances in the arraignment aspects, in the summons aspects, and also in terms of bail and sentencing.

We also, Mr. Chairman, if I may ask you to accept this letter, have a letter which we have received from the New York Civil Liberties Union likewise supporting the aims and goals of NYSIIS.

I would like at the conclusion of my testimony to ask you to consider that for the record.

Mr. GALLAGHER. Very well.

Mr. GALLATI. I also would like at this time to call your attention to a brochure which we have issued and distributed throughout New York State to people in the area of criminal justice, professionals in this field, and to many members of the public entitled "Information Sharing, the Hidden Challenge in Criminal Justice." This describes, I believe, rather well the goals, the aims, and the directions taken by the New York State Identification and Intelligence System. I would ask if you would like to accept this at the conclusion of my testimony, Mr. Chairman. (See p. 159.)

Mr. GALLAGHER. Very well.

Mr. GALLATI. We also have received support from the Association of the Bar of the City of New York, the law enforcement committee thereof, and also the committee on the criminal courts the records of which I would like at a later time to submit to the subcommittee.

We feel that this information sharing capability should be made available to the individual units, which I might add are very numerous, there being 3,600 agencies—separate agencies—of criminal justice in the State of New York, 611 of the 3,600 are police agencies, be they sheriffs, local police departments, city police departments, county police departments, State police, or otherwise—

Mr. GALLAGHER. Do you have machines tied into a network with all of these agencies?

Mr. GALLATI. We will have within the next budget year a total of 40 installations throughout the State of facsimile devices which will provide sending and receiving equipment.

Mr. GALLAGHER. This is a telecommunications system.

Mr. GALLATI. It is a facsimile device attached to normal communications lines, that is telephone or Western Union. We are in the process of evaluating these lines.

Mr. GALLAGHER. What protection do you have against interception?

Mr. GALLATI. We have anticipated the problems of the communications systems, and we are looking very seriously at the devices available such as those used by the military for scrambling and so on, which will permit us to prevent any kind of electronic interception of these transmissions.

Mr. GALLAGHER. Is there such a device now available?

Mr. GALLATI. It is my understanding that there are such devices and that they can be applied to our transmissions.

Mr. GALLAGHER. Is that your understanding, Mr. Baran?

Mr. BARAN. Military cryptographic units are extremely expensive. With the large number of terminals they are eventually talking about, cost could be an overwhelming factor.

Mr. GALLAGHER. What would be your estimate of cost for such a transmission system fully safeguarded against interception?

Mr. GALLATI. We are not able at this time to give you any final costs on that, Mr. Chairman.

Mr. GALLAGHER. Could you give me an estimate for a 40-unit system?

Mr. GALLATI. I can give you estimates of the cost of the units but not of the scrambler, sir.

Mr. GALLAGHER. It is my understanding—and I stand to be corrected—that while a telecommunications system is a relatively simple or inexpensive system to set up, when you start programing, or constructing safeguards the system now starts to multiply from 3 to 10 times. Is that your understanding?

Mr. GALLATI. No; I have not had that understanding exactly.

Mr. GALLAGHER. So we have the benefit of wise counsel, Mr. Baran, is that reasonable?

Mr. BARAN. That seems reasonable. That order of magnitude.

Mr. GALLAGHER. You do not accept that or you do not know who he is?

Mr. LUMBARD. That is right. We do not know who he is or whether he is right.

Mr. GALLAGHER. I know who he is and I know that he has done considerable work on this subject at the Rand Corp., which does some of the big thinking for some of the major problems that confront the military and our Defense Establishment. So he does have some expertise in this department. That is why if you had some information on cost analysis we would be very interested. In fact, I think the Defense Department would find it helpful.

Mr. GALLATI. I do not have it at this time, Mr. Chairman.

Mr. GALLAGHER. This is the key to the whole problem we are faced with.

Mr. GALLATI. I think what I should point out here—and perhaps I am derelict in not having pointed it out before—is that we do have a hierarchy of confidentiality within the system. The Building Block One of which I now speak, which we primarily desire the facsimile devices to support, is a relatively low secrecy type of operation. Perhaps I best might run through the types of things we anticipate having in Building Block One. Let me explain also that it is our concept of development of this system which has been developed at a very deliberate pace, to search out the correct course very carefully through systems analysis procedures and considerable study each step of the way. It is a building block approach and a modular amplification type of building block development. For example, as I said, in Building Block One we will have this facsimile system. The facsimile system is tied in with the other aspects of Building Block One, such as the more rapid response of criminal histories to a fingerprint request, fingerprints having been, in most cases where rapid response is sought, taken as the result of an arrest situation. So we are improving the inhouse turn-around time of the DCI which is now in terms of several days and hopefully it will very shortly be reduced to 1 or 2 days and then to a period of 1 or 2 hours. This is the second module, if you will, of Building Block One.

The third module would be the development of a fraudulent check system. One of the problems of law enforcement in New York State, as I presume it is elsewhere, is the problem of fraudulent checks. Here again, the facsimile system ties in well with the transmission of the fraudulent check from the individual localities throughout the State to a central location where it can be checked to see if the person who has written the check has forged this on other checks and is possible of identification.

Mr. GALLAGHER. How do you identify the caller for the information?

Mr. GALLATI. The callers will have a special code number. When we get into more sophisticated and more detailed security problems, when we go down the road through this hierarchy I speak of in terms of degrees of security, the rank order of security, we will have other devices which we anticipate considering for this purpose. The State of New York is developing a network of closed-circuit television and we feel this will be very helpful to us in terms of our utilization of security measures. The closed-circuit television will permit us to have almost the type of thing that we now have and which so many people and the police feel is so essential; namely, face-to-face confrontation when you exchange information.

Mr. GALLAGHER. You do not feel this can be intercepted very easily?

Mr. GALLATI. Excuse me, Mr. Chairman, I missed the point.

Mr. GALLAGHER. My point is: How do you identify a user or a caller as a bona fide caller?

Mr. GALLATI. No. 1, the agency would be on the system and would have control over the utilization of that particular input-output device which is located in official places such as police stations or courts or district attorney's offices.

Mr. GALLAGHER. Anybody with a proper signal in his cellar might be able to call that information and put it on his wide screen. This is one of the problems that disturbs us. This is why I would like to know your experience.

Mr. GALLATI. We have a coding system which would have to be known by the person who makes the inquiry. He would have a coded inquiry which would then permit him to receive the type of information which he is entitled to receive. The rank order of security, and the hierarchy of the types of things which we will have to provide security for, will begin with limited need for sophisticated security devices. For example, the criminal history sheet which is now available to be transmitted over facsimile machines, or perhaps the fraudulent check which would trigger a criminal history response if the person is identified; this type of information, while it is confidential, is of a relatively low order of confidentiality. It would not be likely that any tremendously sophisticated operations would be involved in trying to intercept this type of information, because it would probably not justify any tremendous involvement of persons who would try to interfere with this. However, we are not overlooking the need for maintaining security both at the point of entry into the system, at the point of reception of the information, personnel security, communication security, physical security, and, of course, actual line security. Again, we are considering this and we will give to each module as it develops the type of security which we feel it deserves in terms of the sensitivity of the material itself and the threat that we have to expect.

Mr. GALLAGHER. Do you have any cost estimates at all on this sort of thing?

Mr. GALLATI. The scrambler which we have looked into was relatively simple and was not tremendously expensive. I do not have the exact figures available at the moment. I would like to make the distinction between the type of scramblers that would be required for very highly sensitive information which could possibly be compromised and which would be of such sensitivity that the threats to it would be so great that it would require these types of tremendous protective devices, as opposed to a much lesser type of protective device which we feel in the Building Block One context, with the type of modules we have on Building Block One, would be adequate for the purposes. I might mention some of the other factors which we anticipate developing as modules for Building Block One. I have spoken of the facsimile system, the development of a more rapid response situation within the division of identification. I have spoken of the fraudulent check module. I would like also to speak of the development of a single fingerprint module, which gives me an opportunity to mention that we have considered in this system the problem of squeezing geography so we have information sharing despite the miles between independent agencies, and we have spoken also of the vertical dimension in terms of the various agencies of criminal justice which all have similar goals and operate in reference to the same types of persons and the same individuals in many cases. I would like to mention also the third dimension, which is one unique to our development, in our opinion; that is, the application of science and technology to developing better operational techniques. We are well aware of the famous computer caveat, GIGO or garbage in and garbage out. We did a system analysis of the problem of latent or scene of the crime fingerprints and we found that these were much less effective than they should be. The public has been lulled into a false sense of security in terms of the utilization of scene of the crime prints by law enforcement people.

Mr. GALLAGHER. This was not the same crooked computer you had in New York, was it, that was used to sell passing marks to police?

Mr. LUMBARD. That is news to me.

Mr. GALLAGHER. I read a story about a person taking a civil service examination and a friend stood next to the computer and put in the right answers. It is one of the weaknesses of the system that I sometimes find. Not only can you take bad information out but you can put the wrong information in.

Mr. LUMBARD. That happened in New York?

Mr. GALLAGHER. It was in the New York Daily News.

Mr. LUMBARD. About a computer in the New York State Civil Service System?

Mr. GALLAGHER. About a computer that was grading civil service examinations.

Mr. LUMBARD. In New York State?

Mr. GALLAGHER. Yes.

Mr. LUMBARD. I would very much appreciate that clipping because that is news to me.

Mr. GALLAGHER. It was news, the Daily News.

Mr. GALLATI. I think we can all agree if you put garbage into a computer you will get garbage out. You do not get anything more

out of a computer in most cases than you put in. Therefore, to merely put more information in a computer and take an ineffective operational technique and magnify that information which is utilized in the operational technique is in a sense multiplying fractions of effectiveness. So we have done a very, very considerable amount of research and study on the problem of scene-of-the-crime prints.

I feel that this is appropriate to call to your attention because I think it does relate to what a computer can do. The Henry system of fingerprinting is now over 60 years of age. It was obviously conceived of and developed long before the age of computers. It is not computer-compatible and it has never served us well as in terms of the scene-of-the-crime prints despite what one might read in detective novels. In order to search a large fingerprint file it is necessary to have a completely visible and readable set of 10 prints from the individual. It is possible in the great bank robbery in England, or the Weinberg kidnaping, to make special efforts to go into your main files. But barring this, the normal procedure for a scene-of-the-crime print is to search it through what is known as a single fingerprint type of system. In New York State where we have I am advised is the largest single fingerprint file of any State in the Nation, we have only 20,000 people in that latent print comparison file, 200,000 individual prints. So if you do not happen to be, as a burglar or a car thief, in that particular file, your chances of being identified by having left a chance impression, anything less than a conveniently rolled set of 10 prints, means that you are "home free."

Only twice in the history of the State of New York has any criminal been so cooperative as to leave us a perfect set of 10 prints.

We have, of course, a very large file in New York State. If we can get into this total file of millions of prints as opposed to 20,000 prints, we are that much better off. I believe that the Federal file is no larger than that of New York State in terms of single fingerprints. So we see the same type of problem at the Federal level. In other words, you have this tremendous number of sets of prints which are not normally searchable and retrievable by any scene-of-the-crime print process, but only by the careful rolling and ink printing of individuals, that is, the normal way in which to assess these files.

Mr. GALLAGHER. Mr. Director, I think I sense an instantaneous retrieval call on me to get over to the House and vote. I think I am going to have to leave. I was hoping that Mr. Horton or Mr. Rosenthal would be back. I would like to say that we appreciate very much your coming down here and giving us the benefit of your experience. We will be happy to include in the record the documents that you have offered.

(The documents follow:)

NEW YORK CIVIL LIBERTIES UNION,
New York, N.Y., March 18, 1965.

Mr. ROBERT R. J. GALLATI,
Director, Identification and Intelligence Project,
Albany, N.Y.

DEAR BOB: Thank you for forwarding copies of senate introduction 1481 and assembly introduction 2625 creating the New York State identification and intelligence system in the executive department. As you know, I have been much impressed by your efforts to improve the processes of criminal justice for many years, and I have been most pleased with the emphasis upon civil rights and liberties which you stressed both as dean of the police academy and in your

field operations. Your continued concern for enhancing civil liberties through computer-based information sharing among the agencies concerned with the administration of criminal justice, in my opinion, is further evidence of your sensitivity to the protection of individual rights.

I fully agree with you that accurate, informed, official decision at every stage of the process of criminal justice will help to safeguard the civil liberties of suspects. Unnecessary arrests and futile commitments can be avoided where adequate data concerning the individual is rapidly available. To the extent that law enforcement becomes more scientific and utilizes sophisticated technology such as you are developing, there will be continually less justification for excessive interrogation and detention prior to arraignment. Where investigative leads and evidentiary material can be supplied or developed through the rapid retrieval of discrete data, it should profoundly improve traditional police practices in the entire area of arrest, search, and seizure.

I wish you well in your sustained efforts to achieve higher levels of professional practice in the administration of criminal justice. On behalf of the Civil Liberties Union let me say that your objectives are consistent with our own and we are delighted to be kept advised of the results of your research.

With best wishes for your continued success,

Yours,

GEORGE E. RUNDQUIST,
Executive Director.

THE VERA FOUNDATION, INC.,
March 16, 1965.

Mr. ROBERT R. J. GALLATI,
*Director, Identification and Intelligence Project,
Albany, N.Y.*

DEAR BOB: Many thanks for sending along the brochure entitled "Information Sharing: The Hidden Challenge in Criminal Justice." It is a highly professional job and should serve to interest a great many people in the benefits to be derived from knowing as much as possible about persons suspected of violating the criminal law.

As you know, Vera Foundation bases its recommendations for summons in lieu of arrest and the release of indigent arrestees on their own recognizance on a rapid research of the individual suspect's reliability. We see the system as a valuable aid in the operational extension of the concepts developed in the Manhattan summons project and the Manhattan bail project.

We are now planning to work in the area of arrests of alcoholics to see if more humane methods of dealing with this problem might prove feasible. Here again, the more one knows about the person with whom he is dealing, the more rational can be the treatment of the individual and the better human rights can be safeguarded.

On behalf of Vera Foundation I would like to assure you that we support your endeavors and endorse the New York State identification and intelligence system objectives so ably presented in your brochure.

Kindest personal regards.

Sincerely,

HERBERT STURZ.

THE NEW YORK STATE IDENTIFICATION AND INTELLIGENCE SYSTEM

INTRODUCTION

The background

As in other areas of the Nation and the world, New York State is in the first stages of a monumental population explosion. In 1960, the population of New York was 17 million. By the year 2000 it will have almost doubled—estimates are at 30 million.

The same expansion that is filling our schools and expanding our economy will, unfortunately, tax our system of criminal justice and correctional institutions. Increased population mobility creates different problems—especially coordination. Today, the average American family moves once in 5 years, or one-fifth of our families move every year.

Some statistics emphasize the effect of the population explosion on the administration of criminal justice. In 1962, in the State of New York:

93,000 lawbreakers were either in direct custody or under legal restraint through probation or parole at any one time.

3,636 agencies concerned with the enforcement of criminal justice were employing more than 66,000 people at an annual cost of \$665 million to local and State taxpayers.

3 million alleged violations passed through the courts of New York, and 700,000 felonies, misdemeanors, and lesser offenses (excluding traffic violations) were reported to the police.

Predictions for the future provide no cause for complacency:

By 1965, 50 percent of the State population will be 25 years of age or under; and statistical studies have shown that the high-violation group consists of persons between the ages of 16 and 25.

Crimes reported are increasing; e.g., 2 years ago, the national crime rate was increasing at four times the growth rate of the population; today, this national rate has risen to five times the population growth.

Fortunately, New York State is somewhat below these national averages, but clearly, there is an urgent social need to combat crime more effectively and efficiently. New tools and fresh efforts are needed; one possibility is for agencies concerned with criminal justice to adapt and employ the resources offered by modern technology in communications and electronic data processing. Just as the general population is more mobile, so is the criminal; criminal activities no longer are confined to a single community or localized area. It is difficult, if not impossible, for local agencies to maintain all files necessary and adequate for their needs. Yet one of the most vital tools in the administration of criminal justice is information—information that may be used as a source of leads in the investigation of crimes, as the basis for preparing criminal charges, as evidence in a court of law, as background for bail and sentencing, and for rehabilitation programs. Under our system of law, information must be utilized at all stages of the process to develop action.

The information problem

Although agencies concerned with the administration of criminal justice have the common goal of protecting the person and property of our citizens, thus maintaining law and order, under the existing structure, each has a separate, manually maintained information system that evolved to suit the purposes and problems of an earlier age. These information files contain many duplications; they vary in scope of content, coverage of individual subjects, format, and currency. When agencies borrow data from each other, the copies and extracts further duplicate and swell the files with a consequent rise in clerical costs and storage space.

The current number of forms in the activity files of State and local agencies concerned with the administration of criminal justice is estimated at 60 million; in 1971, it is estimated that this figure will rise to 70 million. More than 8 million searches of these files are performed annually, and as the crime rate increases with an expanded population, so will the required number of searches.

The State of New York under the leadership of Gov. Nelson A. Rockefeller has taken many effective measures in the war against crime—among the more recent, the establishment of the New York State Identification and Intelligence System (NYSIIS). The concept for this system had its genesis in the investigation of the notorious "Apalachin meeting" in November 1957 of more than 75 of the Nation's top criminals. Even a summary account of this investigation dramatizes the nature of the information problem the system was conceived to solve.

Following the discovery of the Apalachin convention of criminals, the New York State Commission of Investigation was formed in 1958 to undertake an all-out inquiry into the meeting—to identify its attendees and to determine its purpose. Aside from the silence of the meeting's participants, the mechanical tasks of assembling information on these major criminals proved to be formidable: just one of them was the subject of as many as 200 separate official police files in a surrounding area of several hundred miles. Two years later all of the State's files on these criminals still had not been accumulated or assimilated. What the taxpayers had purchased was not brought to bear upon a pressing problem. Those files that were examined often were barren of original material—a relatively meaningless collection of newspaper clippings, copies of other files, and loose notes. The distillation of valuable content was minute.

As chief counsel of the commission, Eliot H. Lumbard was intimately concerned with that investigation and its frustrations. When he was appointed to

Governor Rockefeller's staff in 1961 as special assistant counsel for law enforcement, among the assignments he undertook was a search for possible remedies to the problems presented by the Apalachin investigation, as well as the deluge of papers and files inundating operational agencies concerned with the administration of criminal justice. Out of his inquiries into the possible application of electronic data processing techniques to criminal justice came the New York State Identification and Intelligence System project.

In the last 10 years, the development of new electronic data processing equipment—particularly the electronic computer—has stimulated revolutionary changes in information handling techniques in many fields. Computer-based information processing systems have been developed for military (e.g., air defense) and commercial (e.g., airline reservations) purposes. These computer-based systems make possible the centralized and organized storage of large amounts of data that can then be drawn upon by a network of geographically dispersed user-agencies equipped with communication devices and provide the users access to this central store of information with a speed, accuracy, and un-failing memory unrivaled by any manual methods.

People and plans

In May 1963, Governor Rockefeller, with the concurrence of the legislature authorized a study to determine the technical feasibility and potential significance of applying this new electronic technology to the information problems of the New York State agencies concerned with the administration of criminal justice.

Initial system analysis was performed by the System Development Corp. During this study phase, guidance was provided by the executive chamber and, under the direction of Donald Axelrod, the administrative management unit of the division of the budget of New York State. Throughout the feasibility study, the project derived considerable benefit from a broadly-based advisory committee that met frequently to provide information and advice. Advisory committee members were representatives of—

- The executive chamber.
- The State department of correction, including probation representatives.
- The State division of parole.
- The division of State police.
- The division of budget.
- The judicial conference (the administrative arm of the courts of New York).
- The New York State Association of Chiefs of Police.
- The New York State Sheriffs Association.
- The New York State District Attorneys Association.
- The Office of Probation for the Courts of New York City, and
- The New York City Police Department.

A feasibility report, dated November 1963, resulted from that 6-month study and concluded that a central information processing system was technically feasible and that it could provide valuable assistance to all the relevant agencies.

Governor Rockefeller, in his annual message to the New York State Legislature in January 1964, urged an appropriation to initiate the development and installation of the proposed system. "The increase in the incidence of crime, the modern techniques of organized crime syndicates, and the increased mobility of our population make it imperative that law enforcement officials use the most modern technology in collecting, storing, retrieving, and disseminating information and intelligence and engage in more effective cooperative action in the area of information sharing."

New York State, operating under the system of annual budgets, provided funds for the first year of development. Robert R. J. Gallati, formerly chief of planning of the New York City Police Department, was appointed director of the project. To assist Gallati, Paul T. Veillette, formerly director of the management analysis division of the Chicago Police Department, was appointed technical director, and Paul McCann, formerly director of the division of identification of the New York State Department of Correction, was appointed technical consultant. A growing State staff supports them. The executive chamber, the administrative management unit of the State budget division, and the advisory committee continued to provide support and guidance to the project.

System Development Corp. was selected by New York State to assist with development of the system. A group teamwork approach has been adopted by

New York State and SDC for unified project planning and joint execution of the project.

THE PLANNED SYSTEM

The basic concepts

The New York State Identification and Intelligence System, the first of its kind in the world, has as its long-range goal a computer-based central facility, located at the capital city of Albany, that will store all the information pooled in the system. Qualified agencies concerned with the administration of criminal justice, located anywhere in the State, may contribute and have access to this information center on a voluntary basis via a communication network.

The system's approach is based on the concept of information sharing among all agencies involved in administering criminal justice; these agencies fall into six broad functional groups—police, prosecutors, criminal courts, probation, correction, and parole. These agencies are necessarily independent and autonomous in their operations, yet none of these agencies provides a service that is a totality of and by itself; none functions alone. Each of these agencies has a part in a continuous operation; one subject, and his accompanying file, for example, go successively through these respective agencies until the ultimate disposition of the particular case. With rare exceptions, none of these agencies, except the police, may take official action unless it is on a matter in which another agency has previously acted, and then it is usually concerned with the predecessor agency's "product." Each agency needs to have the same information, with some variations, about each subject, yet each is currently served by separate information sources.

At present, the sharing of information among agencies is uneven in quality; i.e., the transfer of facts often is unsystematic and undependable. A major problem has been the difficulty of developing regular procedures for movement of information among agencies that are involved in different aspects of public service, but are in possession of information of great value were a means for dispensing it to other agencies available.

For example, how is fact "A" in the official files in Buffalo to be correlated with fact "B" in Albany and, perhaps, additional facts in New York City? At present they are not coordinated. Upon full implementation, the new system will provide unified and complete information to all appropriate agencies without compromising the sensitive nature of the information; it will not inhibit their independence of operation, but will provide unity—of information—where unity is urgently needed.

While the system will represent a new agency in State government, independent of all present agencies, it will have no operational powers (such as arrest, prosecution, confinement); it will be strictly a State service agency and will not diminish the authority or autonomy of operation of any of the participating agencies. The system is not a fact-gathering device; it merely makes facts already being gathered by these agencies at taxpayer expense significantly more useful. It is a service tool for these agencies. Its routine functions can be operated effectively by present personnel of the user agencies; the system is basically simple and does not require the creation of an entirely new professional staff or new physical facilities.

There are 3,636 separate and virtually independent agencies that are potential State and local subscribers to the system. Among these are:

Six hundred and eleven police agencies.

Sixty-two district attorneys.

Seventy-five probation agencies.

Two thousand four hundred and seventy-nine courts with criminal interest, including 2,278 justices of the peace.

Four hundred and six institutions for custody and detention.

Three parole agencies.

Selective use of the system can be made by many other agencies, including:

The Waterfront Commission of New York Harbor.

The New York State Department of Motor Vehicles.

The New York State Department of Law.

The New York State Division of Alcoholic Beverage Control.

The New York State Department of Mental Hygiene.

System capabilities

In support of the normal daily operation of these participating agencies, the fully implemented system will provide rapid access to summary criminal history, as well as detailed criminal, social, and modus operandi data on each subject;

will rapidly transmit graphic data, such as photographs and fingerprints, throughout the State; will maintain files of personal appearance data, latent fingerprints, fraudulent checks, warrant-and-wanted notices, stolen motor vehicles, stolen property, laundry marks, stocks and auto registration forgeries; and will provide direct scanning and computer-based searching of all fingerprints on file, arrest and disposition reports, and intelligence information. All of these procedures will be performed with greatly increased scope, accuracy, and efficiency.

The function of fact coordination, with speed, accuracy, and completeness, is the principal contribution of the system in the battle against crime. For example, many advantages are derived from the data files in 1 police agency being immediately available to the other 610 police agencies of the State and to additional agencies performing subsequent activities in the administration of criminal justice. All agencies enrolled in the system, including district attorneys and probation officers, will provide certain types of data in their possession that pertain to their activities and gain direct access to appropriate identification, criminal history, and intelligence files on cases of interest. Courts, correctional institutions, and parole officers may also contribute facts, thus constantly enriching the data base and, in return, make requests of the system for additional necessary information.

However, all types of information would not—in fact, should not—be placed in the central information pool. The advisory committee felt all family court subjects and information should be excluded. District attorneys surely would not place information held in the secrecy of a grand jury proceeding in the system. It is not likely that data such as wiretap information, names of confidential informants, or unverified tips and rumors would be included. The omission of this information, totaling perhaps a fraction of 1 percent of the potential data, in no way affects the value of the entire system.

Data on motor vehicles (except for stolen automobiles and cars owned by major subjects) will not be included in the system because of potential duplication of the data files of the Department of Motor Vehicles system; that material will be readily available through what is called an interface between the two systems. The system will not attempt to duplicate all of the detailed information currently stored in the individual case jacket and folder-files of participating agencies. These files contain considerable detail on particular events, such as indictments, statements of witnesses, daily logs, or detailed descriptions of routine contacts, and parole and probation violations. Such information can be obtained, when it is needed, directly from the appropriate agency's files. However, the system will include adequate references to those sources, such as indications that a subject is currently on probation or parole or is confined in a particular facility.

The installation and operation of the New York State system will make it possible to reduce much of the present duplication of effort among agencies. Because of the duplication of effort, for instance, problems now occur in maintaining current files and in cross-referencing data in different files. These problems can be markedly decreased by an effective concentration of the multiple files into the single file structure of the new system. The system provides, also, for the constant enrichment of the file through mechanisms for updating, deleting, or adding new information. This efficient and appropriate storing and maintaining of data also helps to reduce costs by releasing personnel, space, and resources for other necessary duties.

In summary, the ultimate system as envisaged would provide four major new capabilities. First, suspects from files of known criminals can be identified to a degree and at a speed that has hitherto been impossible. Second, outstanding open cases can be solved by automatic and comprehensive searches that can be conducted on the basis of statewide information. Third, automatic abstracting, indexing, and retrieval of textual intelligence and *modus operandi* information can be used to obtain a comprehensive search of all documents stored in the system and a retrieval of only those documents that are relevant to the interests of the user, instead of the current time-consuming manual index card files and bulky folder files now provided.

Finally, the system offers the tremendous potential of being able to perform research: a pattern analysis of data to assist in evaluating new trends in crime, in testing new approaches to the administration of criminal justice, and in discovering patterns of structure and activity of criminal and special organizations in order to discover relationships in vast bodies of facts that would be almost impossible to develop through standard manual techniques of file searching.

Safeguards

Security precautions will be taken to maintain both the internal integrity of the system and freedom of use by the participating agencies. Interchanges of facts within the system will be made to users on a confidential basis within specific legal, right-to-know and need-to-know requirements. Users will be restricted to a defined category of public officials and agencies. Information will not be available to the general public, subjects of investigation, news media, or private attorneys. If so requested, selective, highly sensitive data will be tagged in the system to insure that its distribution is under the exclusive control of the contributing agency.

Following the commission of a crime, the investigating agency assembles various forms of investigative leads and potential evidence—physical or otherwise—such as testimony. These include latent fingerprints, intelligence data, photographs, handwriting samples, and descriptions of property left at the scene of the crime.

In addition, it attempts to furnish descriptions of the manner in which the crime is committed and, if possible, a description of the alleged criminal. This material, transmitted to the central facility, is compared to relevant files that are stored either in the computer or on microfilm.

If any of these comparisons are successful in providing a match, the system supplies the investigating agency with a list of possible suspects. Upon request, it will provide further specific information that may be stored in this system concerning these suspects.

In addition, the system maintains continually updated information on open cases and stolen property. When the investigating agency arrests a suspect, and if the crime is a felony, the agency prepares an arrest report and a fingerprint card, which are transmitted to the central facility by means of a facsimile transmission device.

There, names and prints are searched for a match with relevant files. If either search is successful, the criminal record is retrieved from the computer and sent to the arresting agency. This agency takes the criminal record together with available intelligence information along with the suspect into court for arraignment and determination of bail.

In the meantime, the system notifies the judicial conference, the court monitoring agency in the State, of the arrest so that the conference can keep track of the court transactions with its own data processing system.

The district attorney begins to prepare his case. He may ask the system for additional relevant information on the crime, including a list of unsolved crimes that resemble the one being prosecuted. If any of the unsolved crimes listed by the computer can be associated with the suspect, they may also become the subject of a prosecution.

If conviction results, the court may ask the probation officer to make a presentence investigation. He may begin his work by obtaining background data on the defendant and on his crime from the system.

If the defendant is sentenced to an institution or put on probation, the appropriate agency registers its custody and any significant events happening during custody with the system. If the offender is placed under parole supervision, a similar process takes place. In this way, the system keeps track of the individual as he moves from one custodian to another and stores this record in the event of any future contact with the State. The data base of the system is thus continually enriched. In summary, a variety of users, each concerned with a particular aspect of the administration of criminal justice, are served by the system.

This system represents a considerable advance in the coordination of relevant facts that, up to now, have not been coordinated and, as a result, are not readily accessible in the complex interrelationships among agencies involved.

The objective of the system is to collect, maintain, and coordinate the maximum amount of relevant data for New York State and local user agencies.

The concept is to provide, through a data processing system, a central store of accurate, complete, and timely information while reducing redundancy and mass of the data and bringing about long-range financial benefits.

SYSTEM IMPLEMENTATION

Building blocks approach

In order to implement the system, a "building blocks" approach was evolved: particular sets of operational capabilities (including the techniques and data) will be produced for the system in modules or blocks; at the same time, system

analysis will proceed on future "blocks" of the total system. This parallel action assures the State of an early operational capability, followed by planned, orderly growth of the system that continuously provides increasing support to the using agencies.

The parallel action plan also permits the system to meet new needs as they arise as a result of changes in the law, user agencies, communities served by the agencies, and in available techniques and ideas. Presently, not all crimes require fingerprints, the system must be prepared to accept the increased load. From time to time, changes in the community require local agencies to perform new or augmented functions; these services, as well as the application of new techniques to the administration of criminal justice, may require additional support from the system.

The approach will utilize a number of long-term research endeavors that come to fruition at different times depending on the complexity of the problems involved; e.g., the system will be ready to utilize direct scanning and classification of fingerprints when it becomes feasible. Through incremental development, each new capability can be integrated with the existing system as the required technology is developed. This organic development focuses new research to support the administration of criminal justice.

The first block of the system is designed to provide capabilities that can only be gained from the sophisticated services of a computer. It will aid in the solution of crimes by providing rapid access to summary criminal histories; the computer complex will supply more information than is currently available from any one agency. Improved communication facilities, including facsimile devices, will rapidly transmit graphic data, such as photographs and fingerprints, throughout the State.

Civil liberties advances

This speed of communication will also realize advances in the protection of civil liberties. Accurate, informed decision by the judiciary will be possible when setting bail or releasing arrestees on their own recognizance; disposition and sentencing, especially of lesser crimes and offenses, will similarly be expedited.

Building block No. 1 will computerize a personal appearance file, a latent fingerprint file, a file of fraudulent checks, and storage and searching of arrest and disposition reports. These capabilities were selected for implementation on a computer on the basis of a system analysis that showed that computerized versions of these files would provide major improvements over the manual techniques in use today. During building block No. 1, the file of fingerprint cards and the name file of the division of identification of the State department of correction will provide major sources of data for the system on a manual basis. Subsequent research and development will lead to computerization of these files with a significant increase in service and efficiency.

Facsimile transmission equipment utilizing present communications facilities will provide user access to the central facility. This network will permit the rapid transmission of textual reports, fingerprints, handwriting samples, maps, photographs, and other forms of data back and forth between the user agencies and the central facility. The goal of building block No. 1 is for the equipment to provide the central facility with sufficiently clear copies of fingerprints to permit classification and matching.

This initial increment of the New York State Identification and Intelligence System will materially aid all the various State and local police agencies concerned with administering criminal justice. A print found at the scene of a crime in a small community could be checked within a short time against the latent fingerprint file in the central facility; a small agency would not likely have an extensive enough fingerprint file. The files of the entire State, then, would be at the disposal of any local community in which a crime was committed.

Similarly, a physical description of a suspect could be compared against data in the central facility; the rapidity and completeness of computer search increases the probability that both large and small agencies administering criminal justice. The system will make possible the communication of an up-to-the-minute summary criminal history to any governmental agency concerned with the administration of criminal justice. The fraudulent check capability should materially aid in the investigation and apprehension of individuals passing fraudulent checks as a result of the speed and thoroughness of investigation made possible by the use of electronic data processing.

Present plans call for the system to become operational with building block No. 1 by mid-1967.

Building blocks 2 and later: Although the full range of capabilities has not yet been determined—special studies are required before specific modules can be selected—there are a number of tentative modules that are likely to be included in the system in the second and third building blocks.

For example, a modus operandi retrieval module is already under development. Modus operandi is one of the more promising types of leads for the solution of crime but, until now, no manual system has been developed that comes close to exploiting its full potential. Computer processing promises a major breakthrough. The New York State Identification and Intelligence System project is engaging in system analysis aimed at achieving a significant improvement in this area through the use of computerization.

A detailed criminal history of each subject would be included in a central file, bringing together selected information now stored in the separate files of the different agencies that contact criminals during the processes of criminal justice. This capability would give every type of agency access to a greater quantity of information than they now have in their own files, thus facilitating the information sharing between agencies that already is necessary. This file, continually enriched from all sources, would cover the history of the criminal's contact with the police, district attorney, court, office of probation, correctional institution, and parole officer, and it would supplement information in the arrest-disposition capability.

Another capability offering great promise would be a fast-response warrant-and-wanted file of those persons who are wanted within the State, including missing persons and persons for whom warrants have been issued. In addition to the police agencies and the district attorneys, courts and parole and probation agencies would be assisted by this capability.

Another module being given high priority for early inclusion in subsequent building blocks is a file of intelligence information pertaining to organizations, people within organizations, and to selected criminals. Organized crime and group-criminal activity, as well as information on subversive activities, would be a special focus of such a module.

Other very useful capabilities will be added. Such areas as stolen motor vehicles, stolen property, property marks, forgeries of automobile registration and stocks and individual social histories as well as scientific data, will be considered. Most of these areas will be planned in the early stages of the system. Considerable system analysis will be required to develop approaches for these modules that may provide important advances over current practices.

THE DEVELOPMENT PROCESS

The production of a complicated electronic data processing system involves many steps: (1) System analysis, (2) system design, (3) production, (4) data conversion, (5) test and installation, and (6) implementation.

System analysis

This initial step will not only provide a detailed definition of the specific needs of the various local and State agencies, but will also spell out the improvement in service that can be provided for the agencies by blending electronic information processing technology with improved manual procedures. Next, detailed requirements for the system will be specified and translated into a suitable plan for development, and finally, a plan for production and implementation of the electronic data processing system will be established. Development of any new techniques that may be required will take place in this phase, also. The following distinct tasks are involved in this total process:

- Analysis of existing system,
- Development of new techniques,
- General requirements for the proposed system,
- Preparation of a plan for the overall system development efforts, and
- Production of system operational requirements.

System design

The general system operational requirements, phrased in user-oriented language, will be subjected to detailed analyses oriented toward computer programming to produce a set of operational design requirements in technical language, specifying those functions and activities to be performed by men and those to be performed by machine. Similarly, organizational requirements to effectively

implement personnel training requirements will be developed. Finally, all of the aforementioned products will be integrated into the blueprints for the system—system design specifications. This document will specify and design the input and output formats and the flow of information both internal and external to the computer. From these system design specifications, detailed program design specifications, defining specific computer program functions, will be prepared.

Production

In this step, the actual information-processing components—computer programs, operating procedures, and implementation handbooks—will be generated. All these components will be subjected to rigorous quality-control testing and debugging (detection and correction of errors). Upon completion of these activities, the nonequipment portions of the system will be available, and actual system installation can begin.

Data conversion

At the same time that the system design and production are taking place, the data conversion (from manual to machine form) will be planned and implemented. In building block No. 1, this will involve the transcription of existing material on criminal history to a computer-readable format for the arrest and disposition module. A selection of fraudulent checks that are currently on file in agencies throughout the State will be made in order to uncover those most likely to be of help in the solution of subsequent crimes. These checks will then be coded according to the technique developed for the fraudulent check module and converted into a form acceptable to the computer. For the latent fingerprint module, a selection of prints will be made of major criminals involved in those types of crime where latent fingerprints are likely to be found. These selected prints will be classified according to the detailed single-print classification system chosen for the module and this, too, will be put in a computer-readable form. It is likely that the personal appearance module will require the establishment of new recording techniques. New forms and techniques will have to be developed and tested, and personnel trained to use them. In order to have a good backlog of personal appearance descriptions when the system becomes operational, all persons arrested for fingerprintable crimes in the State after the technique is available, should be classified according to the new forms.

Test and installation

This step will include the assembling and integrating of system components, as well as extensive system testing. Furthermore, men, machines, procedures, and organization must receive a final integration through experience with the system.

Implementation

This phase is concerned with the orientation of personnel designated by New York State in the use of the electronic data processing system; it also includes preparation of necessary instructional materials.

- The New York State identification and intelligence system—
 - Is voluntary on the part of all agencies;
 - Is not a competing agency; it will have no operational powers such as arrest, prosecution, or confinement;
 - Will not interfere with the necessary autonomy of operation of these agencies;
 - Will minimize the duplication of effort among agencies;
 - Will realize substantial advances in the protection of civil liberties;
 - Will provide unity among the agencies administering criminal justice where unity is appropriate;
 - Will allow new levels of service to the participating agencies;
 - Will make facts commonly used by all six functional areas in the administration of criminal justice readily accessible, as well as certain types of facts especially valuable to particular functions;
 - Will make available, on a "right-to-know" basis, to each individual agency the equivalent of all relevant files in the State;
 - Will contain devices allowing the transmission of photos, prints, handwriting samples, and other material;

- Will have a constantly enriched and updated central data base;
- Will contain in its data base only information used in the administration of criminal justice;
- Will better serve the public interest and better use public funds by the mechanisms it provides for information sharing among the agencies of criminal justice;
- Will be operated by present personnel on premises of user agencies;
- Will be closed to all but a defined category of public officials and agencies; and
- Will maintain security; highly sensitive data will be tagged in the system to insure that its distribution is under the exclusive control of the contributing agency.

IN BRIEF

The New York State identification and intelligence system project was conceived to improve the processes of criminal justice within the State. However, its potential is exciting interest and inquiries from sister States and foreign countries confronted with the same challenges to their existing systems for the administration of criminal justice. It represents an historic event in that, so far as can be determined, it is the first time that every type of agency engaged in the administration of criminal justice has been brought together to think out its common information needs and problems.

Out of this meeting of minds has arisen a pioneering effort to systematically investigate the information needs of all the agencies and to meet those needs by the application of modern advances in electronic information processing technology.

New York State and System Development Corp. are jointly embarked in this effort. Through a mixed-team approach and a tested production methodology, invaluable tools will be developed to aid these agencies in carrying out their responsibilities. When completed, the system will provide faster services to the participating agencies by means of accurate and timely information transmission. The system will permit State and local agencies to substantially improve their information sharing and expand their operational capability.

STATE OF NEW YORK



Print. 5333

Intro. 5104

IN ASSEMBLY

March 18, 1965

Introduced by Mr. DOWD—read once and referred to the
Committee on Ways and Means

AN ACT

To amend the executive law, in relation to the creation of the
New York state identification and intelligence system in the
executive department and prescribing its powers and duties

*The People of the State of New York, represented in Senate and
Assembly, do enact as follows:*

- 1 Section 1. The executive law is hereby amended by inserting
2 therein a new article, to be article twenty-one, to read as follows:

ARTICLE 21

STATE IDENTIFICATION AND INTELLIGENCE SYSTEM

- 3
4 *Section 600. Legislative findings and objectives.*
5
6 *601. Definitions.*
7 *602. Creation of the system; appointment of director.*
8 *603. Functions, powers and duties of the system.*
9 *604. Functions, powers and duties of the director.*
10 *605. Assistance of other agencies.*

EXPLANATION — Matter in *italics* is new; matter in brackets [] is old law to be omitted.

1 606. *Studies; surveys.*

2 607. *Reports.*

3 608. *Grants or gifts.*

4 § 600. *Legislative findings and objectives. The legislature hereby*
5 *finds and declares that:*

6 (1) *The sound administration of criminal justice importantly*
7 *depends upon the effective collection, assimilation and retrieval*
8 *of available information and its dissemination to appropriate*
9 *agencies of government;*

10 (2) *It is in the public interest that, to the greatest extent pos-*
11 *sible, government agencies concerned with the detection, apprehen-*
12 *sion, prosecution, sentencing, confinement and rehabilitation of*
13 *criminal offenders share among themselves available information*
14 *relating to such offenders;*

15 (3) *At this time, relevant information is contained in many*
16 *separate and widely dispersed file systems, manually maintained by*
17 *government agencies throughout the state, and no adequate system*
18 *now exists for coordinating either the files or the information they*
19 *contain;*

20 (4) *There is a need to improve substantially the coordination*
21 *of relevant information and to assure that it is disseminated accu-*
22 *rately and swiftly, especially in aid of police officials, prosecutors,*
23 *criminal courts, and probation, correction and parole officials;*

24 (5) *Through the use of electronic data processing and related*
25 *procedures, a system should be established to provide a central data*
26 *facility, by which relevant information can be coordinated and*
27 *made readily available whenever and wherever required in the*

3

1 investigation and prosecution of crime and the administration of
2 criminal justice.

6 § 601. Definitions. As used in this article:

4 1. The term "system" means the New York state identification
5 and intelligence system.

6 2. The term "director" means the director of the New York state
7 identification and intelligence system.

8 3. The term "qualified agencies concerned with the administra-
9 tion of criminal justice" means courts of record, probation depart-
10 ments, sheriffs' offices, district attorneys' offices, state division of
11 parole, New York city parole commission, state department of cor-
12 rection, New York city department of correction, and police forces
13 and departments having responsibility for enforcement of the
14 general criminal laws of the state.

15 § 602. Creation of the system; appointment of director. There
16 is hereby created within the executive department a New York
17 state identification and intelligence system. The head of such sys-
18 tem shall be a director, who shall be appointed by the governor, by
19 and with the advice and consent of the senate, and shall hold office
20 during the pleasure of the governor. He shall receive an annual
21 salary to be fixed by the governor within the amount available
22 therefor by appropriation. He shall also be entitled to receive
23 reimbursement for expenses actually and necessarily incurred by
24 him in the performance of his duties. The director may appoint
25 such officers, employees, agents, consultants and special committees
26 as he may deem necessary, prescribe their duties, fix their compen-
27 sation and provide for reimbursement of their expenses within
28 the amounts available therefor by appropriation.

4

1 § 603. *Functions, powers and duties of the system. The system*
2 *by and through the director or his duly authorized officer or*
3 *employee shall have the following functions, powers and duties:*
4 (1) *to establish, through electronic data processing and related*
5 *procedures, a central data facility with a communication network*
6 *servicing qualified agencies concerned with the administration of*
7 *criminal justice located anywhere in the state, so that they may,*
8 *upon such terms and conditions as the director and the appropriate*
9 *officials of such qualified agencies shall agree, contribute informa-*
10 *tion and have access to information contained in the central data*
11 *facility, which shall include but not be limited to such information*
12 *as criminal record, personal appearance data, organized crime*
13 *intelligence, fingerprints, photographs, handwriting samples and*
14 *other related data;*
15 (2) *to receive, process and file fingerprints, photographs and*
16 *other descriptive data for the purpose of establishing identity and*
17 *previous criminal record;*
18 (3) *to adopt such measures to assure the security of the system*
19 *as the director deems appropriate;*
20 (4) *to engage in research and make studies and analyses of the*
21 *problems of identification and intelligence and to make the results*
22 *thereof available for the benefit of municipalities and state agencies*
23 *as the director may deem appropriate;*
24 (5) *to do all things necessary or convenient to carry out the*
25 *functions, powers and duties set forth in this section.*
26 § 604. *Functions, powers and duties of the director. The director*
27 *shall be the chief executive and administrative officer of the sys-*

5

1 *tem and shall, subject to rules and regulations approved by the*
2 *governor, direct the work of the system.*

3 § 605. *Assistance of other agencies. To effectuate the purposes*
4 *of this article, the director may request and receive from any*
5 *department, division, board, bureau, commission or other agency*
6 *of the state or any political subdivision thereof or any public*
7 *authority such assistance, information and data as will enable the*
8 *office properly to carry out its powers and duties hereunder.*

9 § 606. *Studies; surveys. In the accomplishment of the purposes*
10 *of this article, the director may undertake research and studies*
11 *through the personnel of the system or in cooperation with any*
12 *public or private agencies, including educational, civic and research*
13 *organizations, colleges, universities, institutes or foundations.*

14 § 607. *Reports. The system shall from time to time report to the*
15 *governor, and shall make an annual report to the governor and the*
16 *legislature, not later than May first, concerning the work of the*
17 *system in the preceding calendar year.*

18 § 608. *Grants or gifts. The director, with the approval of the*
19 *governor, may accept as agent of the state any grant, including*
20 *federal grants, or any gift for any of the purposes of this article.*
21 *Any moneys so received may be expended by the system to effectuate*
22 *any purpose of this article, subject to the same limitations as to*
23 *approval of expenditures and audit as are prescribed for state*
24 *moneys appropriated for the purposes of this article.*

25 § 2. *This act shall take effect April first, nineteen hundred*
26 *sixty-five.*

Mr. GALLAGHER. We would hope that when we have some further hearings on this that your own experiences in this field will have broadened to an extent that will be again even more helpful to us in the future as we consider this problem. I want to compliment you for an excellent presentation. I want to compliment you, too, for your civic spirit in offering to give us the benefit of your advice and of the program that you have instituted in New York State. I think it is extremely useful and will be helpful to us in our future deliberations.

I must run and if you do not mind, our counsel and administrative assistant might have a question or two. Subject to that, the committee would then adjourn.

Mr. GALLATI. I would like to express my sincere thanks to you. You have been most courteous and I appreciate the opportunity of being of any assistance I might have been.

Mr. GALLAGHER. You have been, and we certainly appreciate your appearance.

Mr. GALLATI. Thank you.

Mr. GALLAGHER. For the record, this will be an informal exchange, if you don't mind, with our staff, because theoretically I would now adjourn.

Mr. CORNISH. Is the State Civil Service Commission going to be one of your users?

Mr. GALLATI. The answer to your question, sir, is yes, the State Civil Service Commission would be a user of the NYSIIS file. I might add they are looking forward to this. They anticipate a considerable degree of relief from much of the type of investigation that they now conduct. This type of investigation that they conduct will be assisted by NYSIIS so that a great deal of the annoyance to the civil service applicant will be avoided through getting ready information from NYSIIS.

Mr. CORNISH. Will all applicants for jobs be checked against the system or just certain occupations?

Mr. GALLATI. This would be within the provisions of civil service and appointing officers. We would be recipients of the request. Since it comes from an appropriate source, it would be in accordance with their regulations, the details of which I am not familiar with.

Mr. CORNISH. I think I told you on the telephone the experience they had in the State of Ohio on this where they were checking applicants who wanted jobs as attendants in State mental hospitals in Ohio, and they had a criminal identification center—it was not computerized—at one of the State prison farms. They utilized convict labor as clerks in that office there. Sometimes a request would come in for an identification on one of the old buddies of somebody who was working in the office and they would very conveniently file that one away or put down a negative answer as to his previous criminal record. I assume you are not going to get into any problems like that.

Mr. GALLATI. I can assure you, Mr. Cornish, that we will check out most carefully all those employees that we have working on the system. As a matter of fact, we are now doing so and have done so in the past. This was so even before NYSIIS assumed responsibility for the division of identification. They are very carefully checked for this very reason that you mentioned.

Mr. CORNISH. Individuals picked up as suspicious persons, would they be listed in these records?

Mr. GALLATI. No; definitely not.

Mr. CORNISH. Does New York State law provide in any way that a convicted criminal can become later on, after his supposed rehabilitation, a State employee under any conditions?

Mr. GALLATI. Yes; our provision is in the State law for executive pardons, clemency, and also certificates of relief from disabilities. It is the policy of the Governor to encourage this type of rehabilitative therapy which is involved in employing people who do have backgrounds which have been relegated to a lesser position because of their subsequent good conduct.

Mr. CORNISH. There is some official recognition on the part of the State that a person can rehabilitate himself even though he may be a criminal.

Mr. GALLATI. Yes; definitely. This is not to say on the obverse side of the ledger that the sensitive job should be filled by persons with this type of background.

Mr. CORNISH. You may be interested to know that even in the case of people who have suffered mental illnesses, for example, the Federal Civil Service Commission has been interested in seeing what types of useful Federal employment that some of these people can perform within their limited means.

Mr. GALLATI. It certainly seems like a worthy endeavor.

Mr. CORNISH. In the context of these computer systems these questions have some relevance, as you can well imagine, because the computer system can make a very handy recitation of a person's former record, whether it be a criminal violation or whether it be a mental disorder.

Now, on another subject. You may have covered this earlier when I was out of the room, but did you describe at all your special relationship to the New York City Bar Association study group on privacy?

Mr. GALLATI. I did not go into that directly.

Mr. CORNISH. I think it would be useful if you could give us a brief description of that.

Mr. GALLATI. I would like to, if I may, point out that we have had the privilege of discussing the system with the special Committee on Science and Law of the Association of the Bar of the City of New York, and they have viewed our explanatory movie and listened to Mr. Lumbard and myself describe the system. They responded in a manner which was most helpful to us.

We have had subsequent conferences with members of that committee and also with Prof. Alan Westin, who is engaged as a staff consultant and writer for the committee, and we are attempting to build into our whole context those types of things which they felt were relevant to the proper development of this type of a system. They have been most helpful.

I might add that we have also discussed the system with a number of other people and agencies and institutions who are likewise quite helpful in alerting us to the types of problems we might anticipate. I would like to say this committee will also help to do this very thing for us.

Mr. CORNISH. Any of the suggestions they made, were they worked into this system at all?

Mr. GALLATI. Yes; they are all being taken into consideration and as we develop through the hierarchy, or the rank order, if you will,

of security as we get into more and more sensitive modules, each one of these will be taken into consideration at the appropriate time and given very serious consideration, and we will, of course, make every effort to build these suggestions into the system.

In this formative stage we are now in it is very important for us to get this type of influence because I think we can then overcome this tremendous danger of setting in concrete something which can later not be readily corrected.

Mr. CORNISH. So this liaison which you have with them is a helpful thing?

Mr. GALLATI. It is most helpful.

Mr. CORNISH. The reason I ask that question is, the chairman has proposed a similar liaison between the Bureau of the Budget in the establishment of a national data center, and also persons who would have expertise in questions of constitutional law and the special questions involving invasion of privacy.

I am glad to hear that that association was fruitful.

I do not have any more questions. Perhaps Mr. Romney and Mr. Forsyth do.

Mr. ROMNEY. I have one, Mr. Gallati.

How many employees do you have now working in your system, how many contractor employees, and how many do you expect to have when the system is fully operational?

Mr. GALLATI. We now have on board just a few persons over 300. These are people who are involved in the present manual, to be later computerized, operations of the old division of identification of the department of correction, which we assumed as of April 1 of this year. It includes also more than a hundred people who are involved in a massive data conversion effort.

We are taking the criminal records which are now maintained in manual form and putting these into computerized forms. The effort is tremendous because it is one of the largest data conversion efforts that have ever been undertaken in the State of New York, and perhaps the largest of this type that has ever been done in the world. These people are doing this type of work.

Then we have built up a group of professionals who are on board, State employees systems analysis people. We have with us a topnotch criminalist and we have a number of people who are experts in the field of system design and in terms of analysis of future modules.

And we have beside me here today my executive assistant, also a former member of the New York City Police Department, who is about to receive his Ph. D. in public administration, and has been very helpful in terms of this very area which we are considering today, the area of the right of privacy and civil rights and civil liberties generally.

Mr. ROMNEY. I think you should identify him by name.

Mr. GALLATI. This is Mr. Edward de Franco, also a patrolman of the city of New York on leave like myself.

I think also a point should be made in terms of the reception of the system by the people of the State of New York, and by the officials both in the legislature and in the executive chambers, that we have had a response from the grassroots, and particularly from the people who are in the professional fields with which we will have to deal, which

has been most heartening and perhaps beyond our wildest dreams when we began the system. Their support has been expressed by their representatives in the assembly and the senate who have voted rather substantial budgets for this purpose, and when the bill creating NYSIS, which will be part of the record, was before the assembly and the senate, the vote on that was 57 to 0 in the senate and 127 to 1 in the assembly—and this is in a State which I need not remind you is very conscious of matters relating to the types of things which we are addressing ourselves to here today.

In addition to the State employees which I mentioned, we also have a cadre of seven people from the System Development Corp., who have been with us from the very beginning of the development of the system and who have come along with us and are familiar with all aspects of it.

Among these we have a gentleman by the name of Eric Witt, who is full time, as I said before, assigned to these aspects of development of the system.

The other contractors we have are in the area of data conversion. We have a consultant in this area. Touche, Ross, Bailey & Smart is the consultant we are using in this area. We are using Computer Usage for some of our programming. We are using Jansky & Bailey for the evaluation of our facsimile network and communications matters generally.

We have also employed the technical assistance branch of the Hughes Aircraft Corp. for studies in the intelligence area.

I believe that is the complete list of those who are our corporate consultants, at least as far as I can recall them at the moment.

Mr. ROMNEY. When your system is operational you will have changes of course in your personnel requirement. But do you have an estimate of the personnel that you will be using then?

Mr. GALLATI. We have estimates, but these are of course not truly scientific at this time because it is difficult to gage just what the relationship will be between the savings in terms of manpower by utilizing computerized techniques and the additional pressures we will have to continue to expand on our modular development.

I anticipate, for example, as we develop this single fingerprint capability, instead of receiving as we now do 3 latent prints; that is, 3 scene-of-the-crime prints per week from the entire State of New York, this may be magnified in the order of 50 a week or perhaps a greater number.

Budgetwise, which I mentioned in terms of the support we have had from Governor Rockefeller and the executive chamber and from the "grassroots," expressed in the votes of the legislature, we had in the beginning, in 1963, for the original feasibility study, an appropriation of \$50,000. In 1964, we received an appropriation of \$500,000; and last year we had an appropriation of \$1,250,000. We are now entering the new budget period with a budget of \$3,777,000, for which we are most grateful to the people of the State of New York and to the government of the State of New York.

I think with this type of support we can develop a rational and good system which will serve the interests of the community.

We have, in the area of the support which we have received, another aspect which is less direct but one which we appreciate very

much also. That is in the area of comments we have heard from knowledgeable people in other parts of the world and also from that most sincere form of flattery, which is imitation—a number of States are considering the type of system which we have for their States, and also in terms of scientific reports that we have received.

We recently received such a report from the home office of the United Kingdom in which they refer very flatteringly to the method in which NYSIIS was developed as the most thorough development of computerized systems for agencies of criminal justice they can conceive, and one which they commend for the consideration of the Queen.

Mr. ROMNEY. Is Ohio one of those States?

Mr. GALLATI. I am reminded we are not sure just yet how far or in what direction these systems will go. However, we are made aware of the fact that Ohio is interested in this type of system and may well take the same course we have.

We would like to make, and I think it is important to note, the distinction between some systems which exist of this type in various parts of the United States and our system. Many of these systems that exist in other States are police systems, they are under the jurisdiction of the State police or of the county police department, and they are dedicated to law enforcement, as opposed to the entire spectrum of criminal justice and as opposed to our concept of a totally disinterested agency which has no arrest, investigative, or custodial responsibility.

Mr. FORSYTH. I would like to ask a question on that point. I know you have set up this central system on that concept. Did you have security reasons as substantial consideration when this was done?

Mr. GALLATI. This was one of the reasons.

I think to really answer your question properly, I would have to refer also to the basic common acceptance of the system as a new concept in State government. You do have in New York State—

Mr. FORSYTH. Excuse me. I just wondered if it was a substantial consideration of the setting up of the system independently, for security reasons alone.

Mr. GALLATI. This was a consideration, but I would not say it was the controlling situation. I think perhaps the most substantial reason might be the fact that we did have in New York State, as I assume may be the case in other States, a certain amount of lack of confidence between and among the various agencies of criminal justice.

Mr. FORSYTH. What I am concerned with primarily is the security aspects. Probably it was not really the controlling aspect, a substantial aspect, but you did consider it?

Mr. GALLATI. Yes.

Mr. FORSYTH. Do you think centralizing it increases or decreases security problems it had?

Mr. GALLATI. I think it has decreased the problems of security by centralizing in this fashion.

Mr. FORSYTH. Can you tell me in a few short words why you think it decreases them?

Mr. GALLATI. In the first place, the fact that it was an independent agency, which therefore had no axes to grind, no utilization for the information which was introduced to it other than to properly handle it in the fashion of—perhaps one might use the example of a trustee

who is not utilizing this information for his own purposes but is utilizing it for the people to whom he is responsible.

Secondly, in reference to the amount of security that can be afforded in a central location such as this, the fact that information is filtering in which may be much more sensitive at a local location and becomes less sensitive by removal from the local area, will have a bearing upon it. But, more particularly, I think as you get into an area of larger responsibility, you necessarily will apply more resources to the protection of this responsibility and since the State does have the capabilities and the resources to apply to it, I am sure that we can afford greater security all the way along the line. I keep thinking of Fort Knox as opposed to some drive-in bank. Perhaps this is a bad analogy but I think that we can provide a greater amount and quality of resources to secure the information than can a smaller community which might be limited in its resources.

Mr. FORSYTH. Thank you.

Mr. GALLATI. I might say, of course, NYSIIS is a service agency only. It exists for this purpose, to serve the people who are in the professions related to criminal justice.

Mr. CORNISH. Once again, on behalf of the staff, we want to thank you for staying and answering a few additional questions.

Mr. GALLATI. We are delighted to have the opportunity and appreciate your courtesy and consideration.

(Whereupon, at 1:30 p.m., the committee adjourned. Mr. Gallati later submitted a supplementary statement and additional documents which follow:)

SUPPLEMENTARY STATEMENT OF DR. ROBERT R. J. GALLATI

There is an increasing requirement for greater scientific capabilities and more extensive and sophisticated information sharing among criminal justice agencies within each State. There is also a great need existing in State and local agencies to receive information from the various Federal agencies of criminal justice. Indeed, there is believed to be a great need for Federal criminal justice agencies to share information with each other. Greater capabilities in this area do not necessarily imply greater risk for society; in fact, the opposite may well be true.

The perils we anticipate from large collections of data exist today in our inefficient manual files. It is to the credit of this special subcommittee that these risks are being exposed for rational evaluation. It is also important to recognize that the potentials of computerization have stimulated the concern which exists here today—a concern which is long overdue.

The computer has compelled society to consider the value of security systems applied to information entrusted to data centers, whether they be manually operated, or otherwise. In this moment of truth, the doctrine of the right of privacy has come to share a new place of honor among other protected rights. We need to protect private personality as zealously as we protect private property, for as we protect the right of privacy we protect the right to share and communicate. Surely, privacy protected implies parameters of when, where, with whom, what, how and why information should be shared or withheld. As with all rights, a paramount public interest, accepted by the community and explicitly recognized, should equate, in productive equilibrium, the claim of privacy and the need to share information.

It is within this context of security and a climate of concern for the protection of individual rights and liberties that the New York State Identification and Intelligence System (NYSIIS) is being developed. NYSIIS is a voluntary system of information sharing to serve the agencies of criminal justice in New York State. NYSIIS has no arrest or investigative powers or responsibilities. It is an independent agency created solely to serve criminal justice and to store and retrieve files and forms relevant to the criminal justice process. Thus, information such as contained in census, tax, election, social security, unemployment insurance and similar files would not be collected. We would not expect

that anybody would submit the names of confidential informants, wire tap information, grand jury minutes, etc. It is not planned to include family court information in the NYSIIS data base.

REPORT OF THE SPECIAL COMMITTEE ON PROBLEMS OF LAW ENFORCEMENT OF THE ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK ON PROPOSED LEGISLATION TO AMEND THE EXECUTIVE LAW IN RELATION TO THE CREATION OF THE NEW YORK STATE IDENTIFICATION AND INTELLIGENCE SYSTEM IN THE EXECUTIVE DEPARTMENT, AND PRESCRIBING ITS POWERS AND DUTIES

(S. Int. 3547, Pr. 3960, 5041, Mr. Mangano; A. Int. 5104, Pr. 5333, 6519, Mr. Dowd)

By report dated January 2, 1964, this committee recorded its support of the basic proposition that efficiency and effectiveness of law enforcement will be enhanced by increased cooperation by the various agencies charged with law enforcement responsibilities, and its view that the pooling of information with respect to all matters of concern to such agencies is an activity where such cooperation is particularly appropriate. This report strongly endorsed the feasibility report and recommendations for a New York State Identification and Intelligence System which was designed to utilize electronic data processing equipment for the gathering, recording, and dissemination of criminal intelligence to law enforcement agencies throughout the State.

The proposed legislation (S. Int. 3547, Pr. 3960, 5041; A. Int. 5104, Pr. 5333, 6519) is designed to effectuate the program recommended in the feasibility report. It authorizes the appointment of a director of a proposed New York State Identification and Intelligence System and provides the director with authority to establish a central data facility with a communication network through which law enforcement agencies, as well as other agencies concerned with the administration of criminal justice, can coordinate the collection and dissemination of criminal justice.

This committee believes that the proposed legislation, by facilitating the collection and exchange of criminal intelligence, constitutes a major step forward in improving cooperation among law enforcement agencies, and in thereby improving the effectiveness of law enforcement activity throughout the State. Accordingly, we approve the proposed bills and recommend their prompt adoption.

May 19, 1965.

SPECIAL COMMITTEE ON LAW ENFORCEMENT, THE ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK

Robert B. Fiske, Jr., Chairman.
Arnold Bauman
Edward Q. Carr, Jr.
Arthur H. Christy
Raymond L. Falls, Jr.
Fred N. Fishman
Victor S. Friedman
Grenville Garside
Edwin L. Gasperini
George I. Gordon

David Klingsberg
Stephen P. Kennedy
Whitman Knapp
Newman Levy
Jerome J. Londin
Charles H. Miller
Robert P. Patterson, Jr.
Leonard B. Sand
Leon Silverman
Paul Windels, Jr.

REPORT OF THE SPECIAL COMMITTEE ON PROBLEMS OF THE ADMINISTRATION OF LAW ENFORCEMENT OF THE ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK ON THE FEASIBILITY REPORT AND RECOMMENDATIONS FOR A NEW YORK STATE IDENTIFICATION AND INTELLIGENCE SYSTEM

The Committee on Problems of the Administration of Law Enforcement of the Association of the Bar of the City of New York is of the opinion that the efficiency and effectiveness of law enforcement will be enhanced by increased cooperation among the various agencies charged with law enforcement responsibilities. This committee believes that the pooling of information with respect to all matters of concern to such agencies is an activity where such cooperation is particularly appropriate. Such pooling will eliminate wasteful duplication and at the same time increase the total fund of information available to each

participating agency. The techniques to be employed by the State in the gathering, recording, and dissemination of such information should utilize recent technological advances in data processing. The feasibility report and recommendations for a New York State identification and intelligence system which has been submitted to the New York State executive chamber by the System Development Corp. concludes that a system for the rapid collection, collation, and dissemination of such material from a central electronic data processing system is completely feasible from a technological standpoint and recommends that New York State proceed with the study and system design necessary before such a system may be produced and placed in operation. Although the members of the committee are not competent to pass on the technological aspects of the proposed system, the committee is of the strong opinion that the entire study is well warranted and should proceed with dispatch. We assume that in the course of this study consideration will be given to technological problems and to development of safeguards to preclude any misuse of the system.

January 2, 1964.

Robert B. Fiske, Jr., chairman; Arnold Bauman; Edward Q. Carr, Jr.; Arthur H. Christy; Raymond L. Falls, Jr.; Fred N. Fishman; Victor S. Friedman; Grenville Garside; Edwin L. Gasperini; George I. Gordon; David Klingsberg; Stephen P. Kennedy; Whitman Knapp; Newman Levy; Jerome J. Londin; Charles M. Miller; Robert P. Patterson, Jr.; Leonard B. Sand; Leon Silverman; Paul Windels, Jr.

THE ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK

COMMITTEE ON CRIMINAL COURTS

(1965 Legislative Bulletin No. 12)

(A. Int. 2625, Pr. 2631, Mr. Curran; A. Int. 5104, Pr. 5333, Mr. Dowd; S. Int. 1481, Pr. 1495, Mr. Bush; S. Int. 3647, Pr. 3960, Mr. Mangano)

Identification and intelligence system, creation of within executive department (add new Exec. L. Art. 21).

APPROVED

These bills would create a statewide identification and intelligence system within the executive department.

The bills provide for a director, to be appointed by the Governor with the advice and consent of the senate, and to hold office during the pleasure of the Governor. They would establish a central electronic data processing facility which will receive and disseminate information important in the administration of criminal justice—identification data, criminal records, organized crime intelligence—pursuant to agreements reached with courts of record and the various qualified law enforcement and correctional agencies throughout the State.

The technical feasibility of the proposed system and its value to the relevant agencies were explored during 1963 in a study authorized by the Governor, with the concurrence of the legislature, and were favorably reported upon in November 1963 with many of the agencies being represented in an advisory capacity particularly those in New York City.

Since it appears to be feasible and valuable, we recommend that the system be put into effect as swiftly as possible.

For the reasons stated, these bills are approved.

COMMITTEE ON CRIMINAL COURTS, LAW AND PROCEDURE, THE ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK

Richard A. Green, chairman
Harvey P. Dale
Arthur L. Liman
Irving Mendelsohn
Courtlandt Nicoll
Burton B. Roberts
Francis L. Valente
Thomas D. Edwards
William Scott Ellis
Eleanor J. Piel (Mrs.)

Leonard Reisman
Irving Younger
Edward Brodsky
Malachy T. Mahon
Leon Polsky
Harold Reynolds
Edwin Silberling
H. Richard Uviller
Patrick Wall

(The following material was received for the record:)

STATEMENT BY JOHN DE J. PEMBERTON, JR., EXECUTIVE DIRECTOR, AMERICAN CIVIL LIBERTIES UNION, NEW YORK, N.Y.

The American Civil Liberties Union is grateful for the opportunity to present its views regarding proposals for a Federal Data Center or centers which the Special Subcommittee on Invasion of Privacy is now considering. We applaud the Subcommittee's concern over values threatened by these proposals and the observation by Congressman Gallagher that they raise "serious questions about individual rights."

The implications of such proposals shock the sensibilities of thinking Americans. In our modern age, with all of its intrusive impact on the individual, traditional concepts of a man's right to privacy are already being increasingly undermined. These proposals would alarmingly accelerate this trend.

The privacy of which we speak has been defined in these terms:

"The essence of privacy is * * * the freedom of the individual to choose for himself the time and circumstances under which, and most importantly, the extent to which, his attitudes, beliefs, behavior and opinions are to be shared with or withheld from others." Ruehlhausen and Brim, "Privacy and Behavioral Research," 65 Colum. L. REV. 1184, 1189 (1965).

It is our concern that this privacy, which is an essential source of civil liberties and therefore lies at the heart of our free society, will seriously be jeopardized by proposals presently being made for the collecting and centralizing of all data possessed by the Government regarding each citizen.

We concentrate our comments on two proposals, the FBI National Crime Information Center and the National Data Center.

Under the first proposal, a network of computers would store all information on criminal conduct. Certain valid law enforcement purposes will be served by the creation of such a data center. Police work and crime detection can be more efficiently pursued if information concerning major crimes is readily and quickly available to law enforcement officials. In addition, such a center can serve as a source of vital statistical research on crime and police practices in the United States.

However, two dangers to civil liberties are inherent in the existence of such an information center. The first of these, the widespread use of incomplete and unexplained arrest records, has long concerned the American Civil Liberties Union. We have been deeply troubled by the adverse consequences to an individual flowing from the recording of an arrest not followed by indictment or conviction, as well as from the making of a record of certain arrests, and even convictions, where the true nature of the conduct leading to arrest (such as peaceful participation in civil rights or peace marches) is not disclosed. In our correspondence over the past few years with the FBI about the arrest record problem it has been clearly established that too frequently local law enforcement officials report arrests to the FBI but fail to report later disposition of the case. Countless persons against whom charges have been dropped or who have been acquitted must still suffer the harsh consequences of a wrongful taint of criminality when seeking employment or other privileges. These problems are even more grievous in the all-too-common case today of those arrested for the valid exercise of constitutionally protected rights. No reliable procedure exists for differentiating such arrests in present FBI records from arrests made for the normal incidents of criminal conduct.

The union has frequently suggested methods to eliminate employment discrimination based upon the bare record of an arrest, urged better reporting of arrests and ultimate disposition in each case, and pressed for avenues of legal redress for improper use of arrest records. Yet the problem remains, and will be accentuated by the creation of a central pool of information. Such a pool will serve only to multiply the deprivation of the civil liberties of those who are wrongly arrested or arrested and even convicted for merely exercising their rights. Inaccurate and prejudicial data will be made available to a greater number of police officials and through them to still greater numbers of unauthorized persons.

Our second concern regarding the proposed FBI Crime Information Center is that it will be the repository not just for crime information, which is a valid function, but for other types of information not at all relevant to the prevention and detection of crime. It is said that other Federal investigative agencies will

be invited to feed whatever information they choose into the huge reservoir that the national network of computers will store and retrieve. Data concerning a person's political beliefs and associations, gathered by various Federal security agencies, thus will become part of the crime data bank. The implications are obvious: every local police official will be able to learn with facility not only whether a suspect has a criminal record, a proper disclosure, but also whether he has at all deviated from his community's political or social norms, a highly improper disclosure which threatens the enjoyment of first amendment protections. We know from the history of our own McCarthy era how such information can be improperly used when placed in the wrong hands, to hound people out of their jobs and subject them to other reprisals for their dissenting or unpopular opinions.

We therefore urge that, should such an FBI Center be created, strong safeguards be instituted to insure that only proper or relevant information be stored and that it be used only for proper crime prevention or crime detection ends. Such safeguards should at a minimum—

1. Prohibit the receipt and storing of information other than that formally recorded in connection with the report of a crime and the commencement and disposition of a criminal proceeding.
2. Prohibit the disclosure of such information to any but an authorized officer of a law enforcement agency.
3. Effectively penalize the disclosure by the direct or ultimate recipients of information so obtained to anyone not authorized to receive it in the first instance, and
4. Prohibit the disclosure of any information concerning arrests made more than 60 days preceding disclosure.
5. Provide procedures for the subject individual to learn the whole of the record kept about him, and to compel correction of inaccuracies and prejudicial omissions and the striking of stale records of arrests that have not led to conviction.

Threatening as the proposed National Crime Information Center is, by far the more serious threat to civil liberties stems from proposals to establish a National Data Center whose ultimate design is to centralize in a single place all information possessed by any arm of the government on each individual. We agree with the statement of the chief personnel investigator for the Civil Service Commission that, "Whenever a bureaucracy amasses files about its citizens an inherent threat to liberty exists." In recent years, as our society has incredibly increased and proliferated information gathering about individuals, no person can embark on any of the activities which comprise the essence of modern life, from opening a charge account to seeking a change of jobs, without some investigator prying into his past and present life. In many instances these investigations serve a vital function. But far too often the quest for information expands out of proportion to the actual need. Worse, information relevant for one purpose may be disclosed in the course of a wholly different inquiry as to which it is both irrelevant and prejudicial.

There are two distinct threats to civil liberties posed by the creation of such a data bank. The first lies in the methods by which the information is gathered. Unfortunately, the great bulk of information about an individual is not gathered as the result of inquiries by skilled Government security investigators. Rather, it is often acquired by Government employees of poor judgment, by private agencies, credit unions, insurance companies, and businesses. Government agencies often farm out investigative work to private firms, and there is a considerable interchanging of data among Government and private sources. Once an unreliable bit of information makes its way into a file it forms an indelible mark on a person's record. The individual who is denied the chance for employment or some other opportunity on the basis of such information is given no chance to rebut or disprove it. Dossiers are compiled, the accuracy of which increasingly becomes more questionable. The computerization of such information in the data bank only compounds the basis abuse. Such procedures, taken as a whole, promote a society unresponsive to the necessities of human dignity and privacy, and in the particular case, deny the individual the elements of basic fairness.

The second threat posed by the existence of such a data bank is that information will be used in harmful ways irrelevant to the specific purpose in each case and not intended when the information was gathered. At present each of the numerous Federal agencies that gathered information on citizens maintain their own records for their own particular use. Under the proposed plan, all this information will be centralized. Ultimately, at the push of the proverbial button,

an official from any agency will have access to every bit of data ever accumulated on a person, including information completely unrelated to his concern. For example, information gathered from a passport application will be available to the official processing a request for an FHA loan. Medical and psychiatric histories of applicants for veterans benefits may become available for political misuse. In our view, others simply have no business seeing data gathered for such special purposes. That such access can be abused, and that improper determinations based on legally irrelevant information can be made, is a proved experience with Government. During the 1950's we learned the tragic lesson that the confidentiality of Government files is already too difficult to maintain and that that there are unscrupulous persons who will utilize their access to file information for ulterior purposes.

There is danger that data gathered by the Government will find its way into the hands of private firms where it will be improperly used against an individual. Moreover, the reverse will also occur; thus, for example, a Government agency, itself unauthorized to administer a polygraph test to job applicants, will have available the results of such a test administered to the individual when he applied for employment with a private company. Prohibited results will be achieved in an indirect fashion. When any official determination is made on the basis of irrelevant information which that official has no right to consider, the end result is a deprivation of the individual's civil liberties.

In recent years the Supreme Court has erected constitutional barriers against the improper use of surreptitious surveillance devices (*Silverman v. United States*, 365 U.S. 505, 1961), has prohibited the attempted elicitation by Government agencies of information about an individual's associational ties (*Shelton v. Tucker*, 364 U.S. 479, 1960) and has taken the first step toward defining an area of protected privacy and sanctity into which the Government may not intrude (*Griswold v. Connecticut*, 381 U.S. 479, 1965). The proposed data bank threatens to vitiate these protections so vital to our free society. The content of conversations, monitored by eavesdropping devices, may well be codified and put on tape. The individual's associational ties will become part of his dossier available to the lowest personnel official. The private lives of our citizens, as "documented" by the basest form of gossip, will be fed into the machine. All this in the name of efficiency. This is Government surveillance which brings 1984 to our doorstep.

Confirming our apprehension over the alarming implications of this proposal is the absence, in descriptive statements we have so far seen, of emphasis upon any such vital safeguards as those that have been suggested to the subcommittee by Prof. Charles A. Reich—and the concomitant likelihood that such safeguards will be overlooked in its implementation. Such safeguards would include—

1. Prohibitions on the eliciting, storing, or retrieving by any officer of Government of certain types of information for any purpose.
2. Provision to each citizen of an effective right to inspect the contents of information collected about him and to compel corrections of its inaccuracies and prejudicial omissions, and
3. Limitations on the access to stored information to the original recipient of that information.

The seeming insensitivity of proponents of the National Data Center to the needs for such safeguards underscores the reasons for our opposition.

The principles which protect liberty and human dignity from the insistent demands of order and efficiency are the very stuff of which our democratic society is made. They demand that the collection, storing, and retrieving of essential information, such as that concerning crimes and criminal proceedings, be surrounded with safeguards of the kinds we have proposed. And they demand that all larger conceptions, looking to such essentially unlimited Federal surveillance as that of the proposed National Data Center, be rejected and discarded outright.

We commend the subcommittee for its vigilant attention to these hazards.

PAPER SUBMITTED BY DR. DONALD N. MICHAEL, PROFESSOR OF PSYCHOLOGY AND PROGRAM DIRECTOR IN THE CENTER FOR RESEARCH ON THE UTILIZATION OF SCIENTIFIC KNOWLEDGE, THE UNIVERSITY OF MICHIGAN ENTITLED "SPECULATIONS ON THE RELATION OF THE COMPUTER TO INDIVIDUAL FREEDOM AND THE RIGHT TO PRIVACY"

In this paper, we are concerned with the future—the next 20 years or so. To look even that far ahead may well be a futile exercise, for the rate of change of technology and society threatens to make footless fantasizing of any specula-

tions about the impact of selected factors. However, those who will have significant influence on the political and social processes of the next 20 years are alive today. Consequently, they share to some large degree the values prevailing now, and this is important if we want to explore the significance of the computer for our kinds of privacy and freedom. The years beyond the realm of a 20-year period, may find us dealing with a population a significant proportion of which holds values quite different from today's. Since we are not likely to know what those values might be, further speculations than we are about to undertake would hardly be worth the effort in the context of this Symposium.

One approach to the kind of speculations we shall pursue herein would be to review with great precision and perspicacity the history and ramifications of the concepts of privacy and personal freedom, and in this light, to look at the possible effects of computers on them. We will not follow this approach; space and the author's knowledge are too limited, and the concepts, whether they are refined philosophical, legal, ethical, or political formulations, undoubtedly will have their day when it is time to inhibit or facilitate the impact of the computer. Before then, the impact of computers on man will be reflected much more in the commonplace responses of our pluralistic society to these frequently misunderstood and misapplied concepts. In particular, it should be understood that the writer's grasp of these concepts is also of the "common" variety.

This paper should be read, then, as no more than a stimulus to further speculation and much hard work. It is a preliminary exercise, an attempt to delineate some circumstances where computers and the concepts of personal freedom and privacy may come together in the day-to-day environment of the next couple of decades to enhance or detract from the practice and preservation of freedom and privacy. We shall concentrate on the role of computers as the technological agents for these developments. The microphone, tape recorder, miniature camera, and questionnaire are other formidable technological agents; their uses are well documented in two recent books and we need not review the matter here.¹ We shall be concerned more with the implications for privacy and freedom implicit in the means and capacities of computers for processing and evaluating information, however collected. Our goal is to identify the interactions and the circumstances to look for if we wish to anticipate the impact of computers on freedom and privacy.

In order to grasp fully the potential impact of computers, we must be clear about our versatility. In their simplest forms they can sort punched cards and preform, at high speed, routine arithmetical and statistical calculations. In their more elaborate versions, computers can—

"be built to detect and correct errors in their own performance and to indicate to men which of their components are producing the error. They can make judgments on the basis of instructions programed into them. They can remember and search their memories for appropriate data, which either has been programed into them along with their instructions or has been acquired in the process of manipulating new data. Thus, they can learn on the basis of past experience with their environment. They can receive information in more codes and sensory modes than men can. They are beginning to perceive and to recognize * * *. Much successful work has been done on computers that can program themselves. For example, they are beginning to operate the way man appears to when he is exploring ways of solving a novel problem. That is, they apply and then modify, as appropriate, previous experiences with and methods of solution for what appear to be related problems. Some of the machines show originality and unpredictability."²

Let us also recognize that the impact of computer technology will not be unilateral. Rather, it will be profoundly affected by attitudes held by significant portions of the public and their leaders—attitudes favorable, indifferent, or antagonistic to privacy and freedom. There are, of course, great social pressures already operating which run counter to the preservation of privacy. We shall not explore the sources of these pressures and anxieties; they are recognized as chronic states of mind and action for a large part of our population and its leadership. But they result in conformity and in the justification of exposure, and in order to conform or to assure that others meet certain standards of conformity, people need to know what other people are doing, especially in their less easily observable lives. Our mass media in particular stimulate and cater to this need, and they revel in the publicizing of personalities by stripping

¹ Packard, *The Naked Society* (1963) and Brenton, *The Privacy Invaders* (1964).

² Michael, *Cybernation: The Silent Conquest* 6-8 (1963).

away privacy, whether it be from the individual, his home, the classified senatorial hearing, or the diplomatic conference. There is every reason to believe that defining "reality" in terms of persons and in personal terms will continue, especially as the new, depersonalized reality becomes too complex to convey much meaning to the average citizen. Personalities are meaningful, and defining reality in terms of personalities will continue both to appeal to the conventional wisdom and experience of most people and to provide an attitudinal environment wherein it is more permissible for business and Government to probe persons, too.

Up to the present, "central city" concentration (in contrast to most suburban situations) population growth, and increasing physical mobility have given the individual some relative opportunity to lose himself, or to be anonymous, thereby preserving to some extent his privacy and freedom of action. As we shall see, much of whatever ecological advantage these sources of anonymity provide probably will disappear even if, as is unlikely, the flight to the suburbs ceases.

We must realize, too, that the ways in which the applications of computer technology affect other important aspects of our social environment inevitably will reinforce or overcome attitudes about freedom and privacy. In particular, the computer will have an increasingly significant influence on the design and conduct of public policies. The states of mind and conditions for action resulting from the implementation of these policies will affect the ease with which one can pursue freedom and privacy. An obvious inhibiting influence upon that pursuit would be produced by the siege style of command and control of society which Harold Lasswell calls the "garrison state."³ A garrison state might well be the consequence of an ever more elaborate proliferation of national security policies, guided and embellished by the kinds of computer-based war games, weapons systems, and sophisticated strategies which have become fashionable in the last several years. On the other hand, a federally integrated attack on crime, fully using the ability of the computer to organize and interpret data about criminals and crimes, eventually would free many terrorized people from threats of death or disaster and open business opportunities now preempted by the freewheeling criminal. Thus, it would not be surprising if, in the future, people were willing to exchange some freedom and privacy in one area for other social gains or for personal conveniences. Nor would it be the first time they have done so.

With such background considerations in mind, let us speculate on particular circumstances in which the computer will confront what, in myth or actuality, we take to be present privileges of privacy or freedom.

PRIVACY

Consider that kind of privacy which exists by virtue of the ability to restrict access to information about oneself and one's related activities and records. By and large, the information thus restricted concerns the historical self: not only one's outward conduct, but also his inward evolution as a human being.

The availability of computers can alter seriously the degree to which one can restrict such access. Several factors which have determined degrees of privacy in the past are—

(1) The ability of the privacy invader to bring together data which has been available, but which has been uncollected and uncollated;

(2) The ability of the privacy invader to record new data with the precision and variety required to gain new or deeper insight into the private person;

(3) The ability of the invader to keep track of a particular person in a large and highly mobile population;

(4) The ability of the invader to get access to already filed data about the private person; and

(5) The ability of the invader to detect and interpret potentially self-revealing private information within the data to which he has access.

What is the interplay of these factors and what is their significance for privacy in the light of the computer's capabilities? Much of one's privacy remains undisturbed because no one has had the ability to pull together available information—or because no one has been sufficiently interested to go to the trouble of doing so. To understand the private implications in available data might first require both locating and integrating much widely dispersed information.

³ Lasswell, "National Security and Individual Freedom," 47-49 (1950).

The meaning of the information may be unclear, and, therefore, still private. More information may be needed, and the quality of it may depend on updated surveillance of the person involved. Considering the size and mobility of our society, these problems have made privacy invasion very difficult, but, as we shall see, the computer makes it much more feasible.

Private information about a person may exist which is ethically or legally restricted to those who have a legitimate right to it. Such information, about a great portion of our population, exists in business, medical, government, and political files, and in the form of psychological tests, private and government job application histories, Federal and State income tax records, draft records, security and loyalty investigations, school records, bank records, credit histories, criminal records, and diaries. Each day more of these records are translated from paper to punchcards and magnetic tapes. In this way they are made more compact, accessible, sometimes more private, and, very importantly, more centralized, integrated, and articulated. The results are more complete records on each individual and a potential for more complete cross-correlations. The would-be invader who knows about these centralized or clustered inventories need not search for sources, and therefore he may be much more inclined to examine the records than if a major search for the sources of information were necessary.

As population and mobility increase, there will be other incentives to establish central data files, for these will make it easier for the consumer in new environments to establish who he is and, thereby, to acquire quickly those conveniences which follow from a reliable credit rating and an acceptable social character. At the same time, such central data files will make it easier for the entrepreneur or government official to insure his security, since he will know at all times with whom he is dealing. In consequence, we can expect a great deal of information about the social, personal, and economic characteristics of individuals to be supplied voluntarily—often eagerly—in order that, wherever they are, they may have access to the benefits of the economy and the government.

While this sort of information is accumulating, the behavioral scientist, in direct consequence of the capabilities of the larger computer, will be improving his ability to understand, predict, and affect the behavior of individuals and groups. For the computer provides two prerequisites for the development of effective social engineering. First, only the computer can process fast enough the enormous amounts of data needed to know what the existing states of social and economic affairs are. In the past, such information was scanty or non-existent, or what there was more or less out of date. This no longer need be; and it certainly will not continue to be, since coping with sheer social complexity will require that such information be abundantly available. In the second place, the computer will let the social scientist manipulate enough variables and enough circumstances in sufficiently complex ways to invent subtle models about the behavior of man and his institutions. Simulation of the behavior of individuals and institutions through the use of computers is well underway, and all signs are that it will be exceedingly productive. There is every reason to believe, then, that with the development of these sophisticated models, and with access to centralized data banks where many of the characteristics of each person, the institutions with which he is involved, and the environment in which he operates are recorded, it should be possible to develop a sophisticated understanding of the present behavior of individuals and to predict with some assurance various aspects of their future behavior as well as to interpret and deduce aspects of their past behavior. How detailed and valid the conclusions will in fact be remains to be seen, but it is very likely that average citizens, as well as those who will have a vested interest in using such predictions, probably will overestimate their precision. Even today, many people are willing, indeed sometimes want, to believe that the behavioral scientist can understand and manipulate their behavior. Whether the ability to predict behavior will be used to invade privacy and freedom will depend on more than technological capability, but certainly the capacity for invasion will increase as behavioral engineering progresses.

The ability of the user of private information to gain access to already collected data about the individual will depend on several factors. To understand the range of possibilities it should be recognized that, increasingly, data will be stored in memory banks shared by several users. A computer's memory banks can be so large that only a relatively few users can employ their entire capacity. Furthermore, the speed and capacity of computer processing is so high that it is much more efficient to have several users sharing time on

the machine. This means that while one user's finger is moving toward a control button on his computer control panel, another person is using the circuits he will be using a few seconds later. In the future, one computer user might accidentally gain access, through equipment malfunction, to another's information stored in shared memory banks. It is also possible that such information could be retrieved deliberately and clandestinely by querying the computer with someone else's retrieval codes or by otherwise tricking the computer and its memories. Shared computer time and shared memory banks are new techniques, and the possibilities for their abuse will become fully apparent only with extensive use—and misuse. Of course, one information user, through legitimate means, could gain the use of information in another organization's memory. Certainly, governmental interagency cooperation is inevitable. This is likely to occur also in some forms of interbusiness cooperation. As computers are interconnected more and more, as related organizations come to share specific memory banks, the inclination to share information and the ease of doing so will increase. After all, one of the advantages of the large-scale use of computers is the savings to be made by eliminating duplication of information and by standardizing information collecting forms and data retrieval languages.

So far we have speculated on the increased opportunities which the computer provides for invading privacy from "outside" the person. But there are trends which suggest that many people are likely to cooperate in exposing their previously private selves. Systematic exposure of the private self through questionnaires, interviews, and test taking is becoming steadily more widespread and probably more acceptable. The pressures toward—indeed, the attractiveness of—this kind of exposure are strong. In the first place, many Americans like to believe that getting ahead is a matter of ability and personality rather than luck or nepotism or some other kind of whimsey in those who hire and fire them, or in those who acknowledge or ignore them when opportunities arise. As the society grows more complex and the individual's sense of his ability to influence it in his own interest seems smaller, the tendency to depend for placement and advancement on what can be revealed about oneself which can be evidenced and acted on "scientifically" may well increase. This would be a natural extension of our dependence on the expert, for it will be the expert who will assess one's "true" value—at least one's economic value—by evaluating the private information one makes available about oneself. This response also will be a natural extension of our dependency on the machine, which in this case will help the expert or make the decisions itself about the value of the individual, impersonally but with great precision, on the basis of what it knows. And the machine will do so "privately": it will not blabber secrets to other machines or other people.

Complementary pressures from those who would use information about the private person are likely to be great. The real or imagined need to use people efficiently will increase as more organizations find themselves in the throes of complicated and disrupting reorganization, remodeling people and procedures to meet requirements imposed by the use of automation and computers. Thus executives and decision makers, responding to emotional and practical pressures, will try to squeeze the utmost from available personal information as clues to efficient job assignments. Increasingly, executives seem to seek security through technological intervention in the conduct of their activities. This tendency will be reinforced as more executives become the products of physical or social engineering backgrounds. As the behavioral scientists' predictive capabilities are increasingly recognized, and as business and Government become more professionalized and rationalized through the combined impact of the availability and capabilities of computers and the hyper-rational orientations of the personalities who tend these devices, management will seek more and more to learn all it can about the people it uses and about the people it serves, in order that its tasks may be more efficiently conducted in the public interest or in its own. This is, of course, simply a continuation of a well-rutted trend. For some years we have assumed or accepted that efficient Government, Government subject to as little internal disruption as possible, "requires" personnel selection on the basis of very private information about an applicant's sex life, family affairs, and early ideological enthusiasms. Since most new jobs in the past two decades have been Government or Government-related jobs, we can expect this trend to continue, the result being that more people than ever will be on file.

We have noted the likelihood that, as the years go on, the pressures will increase substantially to collect and use available data about the private individual, to enlarge the scope of that data, and to attempt to correlate and expand its implications and meaning. To some extent, each user of information will gather his own, but, in keeping with standards of efficiency, there will be efforts to gain access to data accumulated by others. For example, we can expect pressures to combine credit rating information with Government job application information, with school psychological testing information, and so on. In an enormously complex society, everyone may have something to gain by this process as well as something to lose.

One thing is clear: for a long time indeed no correlation of data will account fully for the personality being evaluated and interpreted. Whatever the person providing the information believes, and whatever those using the information believe, there still will be a truly private person left, undetected by the computer. This is not meant in any mystical sense. It will take much longer than the 20-year period we are dealing with to gain enough understanding of human beings truly to strip them of all the private self which they think they volunteer to expose. Nevertheless, in many situations, that information which can be processed through punchcards or memory tapes will be accepted as the important private profile of the individual. This will be so because, limited as the data may be in some abstract sense, this will be the information most conveniently available to the users for the assessment of the individual. And it will not be trivial or simple information. It will be impressive in its scope, and the computer will be impressive in the processing of it. Thus the users will choose to believe that this is the important part of the private life of the individual, and from the economic standpoint it may well be. Similarly, many of those supplying the information will come to believe they are revealing their private selves. In other words, that which will be valued and acted on as if it were the private individual will be that which can be tested and assessed in ways which can be recorded and manipulated by computers. Of course, not everyone will succumb to this bifurcation of self, but enough may do so to make it an important factor in our society. The result may be that many will feel they or others have no private lives. Others will feel that their "real" private lives are even more private because they are relatively more ignored—the computer won't be able to do anything with them. Thereby we shall have a new measure of privacy: that part of one's life which is defined as unimportant (or especially important) simply because the computers cannot deal with it.

No one using the output from a computer needs to know as much about the data fed into it as does the programmer. Without intimate and extensive understanding of the data and the uses to be made of it, the programs which determine how the computer operates, and hence the quality of its output, will be crude. On the other hand, executive decisions often depend less on knowledge of details than on overall grasp of the situation. As a result, the programmer often will be the person with potentially the most intimate knowledge of the private lives of those whose data is processed. This potentiality need not result in his having specific knowledge about specific people, since a programmer is unlikely ever to see the materials which are input to the computer whose processes he has arranged. But given his deeper understanding of how the data are being processed, what assumptions are made about the relationships among the data, what constraints must be put on the data in order for the computer to use it, it is entirely possible that the programmer may be called upon in difficult cases to enrich the executive's basis for decision making. In this way, the programmer may become privy to very private information about specific individuals. There may then arise a demand for programmers with ethical standards which now are not considered prerequisites to their trade. Inevitably, of course, there will be corruptibles among this group who will leak private information.

In another sense the programmer will become important for the preservation of privacy and freedom. The way he arranges the relationships in the information to be processed and the relative emphasis he gives to different items could result in distortions in the "history" of the person and, hence, in the implications of the data. In other words, the programmer could invent a private life. The question then arises of how the individual protects and asserts his own version of his private life over and against that defined by the computer. In the past, it has been possible to refer differences in present interpretations of past events to witnesses or paper records or photographs. Such records were public in that they were visually comprehensible. But records storage will

become ever more bulky and retrieving information will become an increasingly awkward and vexing task as the population increases and as the amount of information about each member of the population increases for the reasons we have discussed. The incentives to put this information into computer memories will thereby increase. But if history is recorded on tapes, in magnetic codes, and on molecular films, the definition of what was will become ever more dependent on how the machine has been programed and what it is able to retrieve from its memories. As respect for and dependence on the computer increases, it is likely that respect for and dependence on fragile and "ambiguous" paper records will decrease, lessening the ability of the individual to establish a past history different from that jointly provided by the programmer of raw data and the interpreter of processed data. There will be fewer opportunities to derive a public consensus on what the data "is," for there will be no public language in which the primary data will be recorded through which the public can verify the meanings and facts of the records. Robert Davis of the Systems Development Corp. compares this situation to the time when the Bible was interpreted to the illiterate, and what the Bible said and meant depended exclusively on what those who could read claimed it said and meant.⁴

On the other hand, centralization of private information and its preservation in computer memories may decrease illegitimate leaks of that information. Those who will have access to personal history will see much more of it than was usually the case when it was contained in printed records, but fewer curious eyes will have knowledge of any part of the private history of the individual.

PERSONAL FREEDOM

Now let us look at a few possible confrontations between the freedom of the individual and the computer.

There is one form of technology tied to the computer which today increases freedom for some and which may in the future decrease it for others. This is the technique of telemetering information from tiny sensors and transmitters embedded in the human body. Right now, one form of these devices keeps recalcitrant hearts beating steadily. In a few years, in variations of already existing experimental devices, they will transmit information about subtle internal states through a computer to the doctor, continually or at any time he wishes. Clearly, the lives and liberty of people dependent on such support will be enhanced, for it will provide greater opportunity to move and to live than would be theirs if this information were not so continuously and directly available.

It is not impossible to imagine that parolees will check in and be monitored by transmitters embedded in their flesh, reporting their whereabouts in code and automatically as they pass receiving stations (perhaps like fireboxes) systematically deployed over the country as part of one computer-monitored network. Indeed, if they wish to be physically free, it is possible that whole classes of persons who represent some sort of potential threat to society or to themselves may be required to keep in touch in this way with the designated keepers of society.

It may seem farfetched to suggest that such people might walk the streets freely if their whereabouts and physiological states must be transmitted continually to a central computer. But two trends indicate that, at least for those who are emotionally disabled, this is not unlikely. We are now beginning to treat more and more criminals as sick people. We are beginning to commit them for psychiatric treatment rather than to jail. This treatment may have to continue indefinitely, since frequently a psychiatrist will not be prepared to certify that his patient will not commit the same kind of crime again (as is now required for sexual offenders under psychiatric treatment). At the same time, chemical and psychotherapeutic techniques for inducing tranquil emotional states are likely to improve. We may well reach the point where it will be permissible to allow some emotionally ill people the freedom of the streets, providing they are effectively "defused" through chemical agents. The task, then, for the computer-linked sensors would be to telemeter, not their emotional states, but simply the sufficiency of concentration of the chemical agent to insure an acceptable emotional state. When the chemical agent weakens to a predetermined point, that information would be telemetered via the embedded sensors to the computer, and

⁴ Interview with Robert Davis of Systems Development Corp., in Washington, D.C.

appropriate action could be taken. I am not prepared to speculate whether such a situation would increase or decrease the personal freedom of the emotionally ill person.

Already the computer is being used in conjunction with other technologies to retrieve information customarily stored in libraries. Doubtless, this use of the computer will expand greatly. Tied in with telephone lines and television cables, it will make it possible to gain access to vast areas of knowledge without leaving one's own local area. To the extent that knowledge increases the individual's opportunities for growth and effective mobility, we could say that such access at a distance will increase his freedom. This will be especially true for those who do not live near the conventional repositories of information.

It is sometimes suggested that the computer will bring back townhall democracy by making it possible for every voter to express his opinion at the time his representative needs it, merely be a pushbutton response to a teletyped or mass-media-transmitted request for the constituent's position on a given topic. The voter would gain more freedom to express himself, but that of the representative to act in terms of his own estimate of the best interests of the Nation or his district might be lessened by such ubiquitous and massive grassroots expression. If the representative were able to determine the voter's understanding of the issue in order to assess the meaning of his pushbutton vote, however, and if he had information on voters so that they could be clustered according to background, thereby allowing patterns of votes to be more fully interpreted, the representatives' ability to act in the combined interests of his various constituencies and the Nation at large could be increased. Such data also would give him a better basis for providing his constituents with the information they need in order to vote more intelligently. The biggest unknown would seem to be whether one could count on developing an intelligent and enlightened public, or whether computers used this way would simply increase the likelihood of representatives being swayed or dominated by a mass incapable of judging the meaning or implications of the complex issues it is asked to evaluate.

If it is worthwhile, the enormous capacity of computers can provide the basis for differentiating among many subpopulations. This capability could mean increased responsiveness on the part of data users and planners to the different social, psychological, and material needs of each of these populations. It could lead to more opportunities for individual expression, at least to the extent that the substance of individual expression is significantly differentiated by membership in various subgroups. In this sense, the computer could provide a greater opportunity for freedom than would be available in a large society which had to plan and operate in terms of overall averages rather than differentiated averages. But this capability for recognizing differences in populations and interest groups could also be applied to more detailed surveillance, causing a much greater loss of freedom than would result in a large population dealt with in overall averages. In the latter situation, the individual could more easily lose himself in the mass.

Behavior is internally mediated by the individual's history, personality, and physical capabilities, and externally by the constraints which environment imposes or the opportunities which it provides. Knowledge of external environmental characteristics increases the observer's ability to predict individual behavior. This is evidenced by the ability of police, military intelligence, or traffic control experts to predict, from knowledge of their environments, likely behavior of specified people or groups. Obviously, these predictions are improved greatly when added to knowledge of the environment is knowledge of the typical response of the individual to similar environments. The police capturing the criminal when he returns to the scene of the crime, the successful guerrilla ambush, the parent removing "temptation" from the child's environment, and the "lead item" between environment and individual behavior toward it can be used to predict and channel that behavior. Better predictions about behavior should be possible when external environment can be codified and defined in much greater detail by using computerized data and by using the computer to detect patterns of sequences and arrangements of individual acts through elaborate analysis and synthesis of the data. The resulting predictions could be used to alter an environment (inanimate or human) in order to provide more opportunities for alternative behavior to facilitate habitual behavior, or to inhibit or terminate behavior.

As usual, the consequences of environmental controls for freedom could go either way. Improved surveillance techniques would mean less crime, or, at any rate, less than there would be without such techniques. Less crime means more freedom and privacy, at least for the law abider. But the same techniques could be used against the law abider if his Government wanted to make, say, a routine security check in the interests of social stability.

When the application of computers requires that people change their behavior toward something familiar, they may well interpret this as an imposition on their freedom. This interpretation is in keeping with the belief long held by many that the machine is the chief threat to the spontaneity (freedom) of man. The recent furor over all-digit dialing demonstrates how seriously this threat is taken.⁵ In the abstract, at least, one's freedom to dial long-distance numbers direct may be increased by this new system, and certainly it is not lessened compared to what it was when one used a mixture of letters and numbers. But obviously many people feel their freedom has been abridged because for them it seems easier to remember combinations of letters and numbers, and because this change symbolizes more mechanization and, thereby, a challenge to the freeman. Undoubtedly, there will be further "invasions" of this sort.

An important variant of this state of mind is found in responses to the nationwide computerized system which makes it possible for a cashier to determine quickly whether an unfamiliar person seeking to cash a check has a criminal record. Through this system (cashier to computer to police) a number of criminals have been apprehended while they waited for their check to be cashed. Abhorrence of the system and sympathy for the bum-check passer is a common—although, of course, not unanimous—response to descriptions of this system in action.

Apparently, in many minds there is combined a sense of "There but for the grace of God * * *" and a realization that the inclination to violence and law-breaking which most of us harbor) will be throttled more and more even in fantasy. For what is mere man against the implacable, all-seeing machine? The godlike omniscience of the computer essentially destroys his hope, and hence his freedom to fantasy, that he can get even unfairly with a society which he thinks has been unfair to him. If the computerized world of tomorrow produces the kinds of rationalized standards which increase one's frustration and inhibition, then certainly this invasion of one's right to hope (i.e., to fantasy antisocial success) will be interpreted as some kind of invasion of his personal freedom. If so, there most certainly will be an acceleration of a trend already underway: "Frustrate" the machines. In a spirit of desperation and vengeance people are bending punchcards, filling prepunched holes, and punching out additional ones. (Injunctions have already made it clear that this destruction of private property will not be tolerated, regardless of its contribution to the preservation of psychic property; the machine wins.) They are also overpaying, by one cent, computer-calculated and computer-processed bills and refusing to use postal ZIP codes.

Now, it may well be that existing law or future decisions and actions of courts and legislatures will enforce and elaborate present legal powers in order to conquer the threats to freedom and privacy on which we have speculated. But seldom is a law promulgated in anticipation of problems, especially when there are powerful interests which benefit from freedom to exploit. Moreover, as we have seen, in most cases there may be a potential or actual gain for freedom or privacy along with the loss. And as we well know, even existing laws protecting privacy and freedom are often difficult to apply ubiquitously and effectively. In the hothouse world of Washington, D.C., it is commonly believed that anyone who is anyone at all has had or is having his phone tapped by Government agents. Whether or not this is true, what is important is that people believe it is true, and they accept this situation feeling either that the Government has a right to such spying or that, even if it hasn't, they can do nothing about it. We are all well aware of the increasing pressures to enlarge the search and arrest powers of the police in the face of expanding urban crime. We know, too, that in some places some of these powers have been granted or their unsanctioned use tolerated. And what shall we occlude about such modifications of the law as that represented by an executive order which gave the House Committee on Un-American Activities for the period of the 88th Congress

⁵ See, e.g., Time, July 13, 1962, p. 53; Washington Evening Star, Jan. 31, 1964, p. A12, col. 2.

the right of access to any income, excess-profits, estate, or gift tax records it wished concerning subversives?⁶

In the face of the increasingly complex tasks of maintaining, to say nothing of improving, urban society; in the face of general popular disagreement at best, and indifference at worst, about the proper conduct and protection of the individual in this alienated and splintered world; in the face of the special advantages the computer provides to increase information, command, and control—I would speculate that, at least for some time to come, these advantages will generally be considered more important than protection or preservation of those threatened aspects of freedom and privacy we have examined here.⁷

⁶ Executive Order 11109, Fed. 11109, 28 Fed. Reg. 5351 (1963).

⁷ I am indebted to David T. Bazelon, Robert Davis, and Patricia McMonigle for their suggestions during the preparation of this statement.

...

APPENDIXES

APPENDIX 1.—REPORT OF THE COMMITTEE ON THE PRESERVATION AND USE OF ECONOMIC DATA TO THE SOCIAL SCIENCE RESEARCH COUNCIL, APRIL 1965

MEMBERS OF THE COMMITTEE ON THE PRESERVATION AND USE OF ECONOMIC DATA

Richard Ruggles, chairman.
Richard Miller, secretary.
Edwin Kuh, Massachusetts Institute of Technology.
Stanley Lebergott, Wesleyan University.
Guy Orcutt, University of Wisconsin.
Joseph Pechman, Brookings Institution.

SUMMARY OF REPORT

During the past four years the Committee on the Preservation and Use of Economic Data has met with a considerable number of Federal agencies concerned with the collection and use of data in machine readable form. The prime concern of the committee has been the development and preservation of data for use in economic research. Although considerable progress has been achieved in specific areas, the committee has concluded that three more general lines of action are required. Specifically, these are (1) the Federal Government should undertake the establishment of a Federal Data Center; (2) procedures should be established to insure the development and preservation of import data; and (3) research institutions and universities should develop an organization for coordinating their requests for economic data.

First, the committee urges that the Bureau of the Budget, in view of its responsibility for the Federal statistical program, immediately take steps to establish a Federal Data Center. Such a Federal Data Center should have the authority to obtain computer tapes and other machine readable data produced by all Federal agencies. It would have the function of providing data and service facilities so that within the proper safeguards concerning the disclosure of information both Federal agencies and users outside of the Government would have access to basic data. The Federal Data Center would require computer facilities, and it would need to be staffed with personnel capable of understanding the data problems in the various areas. In view of the importance of the Federal Data Center, the committee suggests that the Center be established with specific responsibilities for these functions and interagency authority to carry them out.

Second, the committee urges that the Office of Statistical Standards of the Bureau of the Budget place increased emphasis on the systematic preservation in usable form of important data prepared by those agencies engaging in statistical programs. In both the initial budget for statistical programs and the subsequent review of ongoing work, the Bureau of the Budget should see that provision is made for the development of computer tapes of important data, together with the supplementary material required for interpretation.

Third, the committee recommends that at an early date the Social Science Research Council convene representatives from research institutions and universities in order to develop an organization which can provide a clearinghouse and coordination of requests for data made by individual scholars from Federal agencies. In addition, such an organization would serve the Federal Government in an advisory capacity and provide a mechanism for the development of data tapes needed for research purposes in specific areas of economic research.

The Background and History of the Committee

In December 1959, the executive committee of the American Economic Association devoted a part of its annual meeting to the consideration of the preservation and use of data for economic research. The AEA Executive Committee recognized that research in the social sciences in general, and in the discipline of economics in particular, to an increasing extent requires large systematic collections of microdata for the formulation and testing of hypotheses, and that collections of microdata are research tools for the social scientist much in the same way that books and manuscripts are for the humanities and laboratories are for the scientist.

Although the AEA Executive Committee agreed that the problem of developing and preserving important bodies of microdata was extremely important, they concluded that it was not feasible for the American Economic Association to undertake an effort in this area, since the organizational structure of the association makes it difficult for subcommittees to carry out substantive work of this nature. The executive committee therefore recommended that the Social Science Research Council set up a Committee on the Preservation and Use of Economic Data to study this problem and undertake any program of action which it might deem desirable.

CREATION OF THE SSRC COMMITTEE

Accordingly, in December 1960 the Social Science Research Council arranged an exploratory discussion of the problem of data preservation and use, drawing on social scientists from universities and the Federal Government. This discussion revealed that although there was a large area of common interest among the various social sciences, there were also wide differences in approach and areas of concern when any specific aspect of data preservation and use was being considered. It became obvious that the problem was too broad and diverse to be solved by any simple general solution, and that a more concerted and focused attack on specific parts of the problem would have to be undertaken.

For this reason, a small committee was then appointed to explore the problems arising in the field of economic data alone. This committee consisted of individuals who were acquainted with the statistical work being done within the Federal Government, and who were also doing research using large bodies of empirical data. At the outset the newly constituted Committee on the Preservation and Use of Economic Data recognized that in order to maximize the effectiveness of its effort it should concentrate its attention on those areas which would yield the most valuable research materials per unit of cost. By definition this immediately excluded information which was widely scattered throughout the Government or stored in bundles in warehouses, and it suggested that attention should be focused on those bodies of information which were currently available in machine readable form. The Committee was concerned with the archival problem, as well as the problem of making existing data currently available to research workers, and for this reason it proposed to examine the disposal policy of the various Federal agencies as well as to try to develop methods whereby machine readable data could be made directly available to scholars engaged in economic research.

COMMITTEE ACTIVITIES, 1962-1964

During the 3 years from 1962 through 1964, the Committee undertook to study, on an agency-by-agency basis, the problem of providing access to specific bodies of information. Meetings were held with a considerable number of independent agencies in the Departments of Commerce, Labor, Treasury, Agriculture, Interior, and Health, Education, and Welfare. In addition, the Committee kept in close contact with the Bureau of the Budget and the National Archives. In some cases, arrangements were made to create and make available specific bodies of information, and substantial progress was made in developing awareness of the general problem of preservation and use of data by the Federal agencies. Representatives of the National Science Foundation attended many of these meetings.

Despite the progress which was achieved in specific areas, however, the Committee, at the end of 3 years' operation, concluded that some more general solution was required. Such a solution would require that the Federal Government develop (1) a systematic policy insuring the preservation of important data, and (2) mechanisms whereby data could be made available for research pur-