the applicable base period (as those terms are defined in subsection (e)). If he determines that the price index had changed by a percentage (of its level in the base period) equal to 3 per centum or more, the amount of the educational assistance or subsistence allowance payable to eligible veterans or eligible persons pursuing a program of education or training, other than a program by correspondence or a program of flight training, in an educational institution under chapter 31, 34, or 35 of this title shall be changed by the same percentage (adjusted to the nearest one-tenth of 1 per centum), effective with respect to such allowances for months after the quarter in which the determination is made.

"(b) In the case of any individual who first becomes entitled to an educational assistance or subsistence allowance in or after the month in which a change becomes effective under subsection (a), the amount of such allowances payable to or with respect to him on the basis of such entitlement shall be determined by applying such change (or, if more than one change has become effective under subsection (a), by applying all such changes successively) to the amount of such allowances which would be payable under the provisions of chapter 31, 34, or 35, as the case may be, without regard to this section.

"(c) Any change under subsection (a) shall apply with respect to all educational assistance or subsistence allowances payable under chapters 31, 34, and 35 of this title during the period in which such change is effective regardless of the provisions under which such allowances are payable or the manner in which the amounts payable are determined, but shall be applied with respect to the allowances payable to or with respect to any particular individual only after all of the other applicable provisions of this title which relate to eligibility for and the amount of such allowances, and all prior changes made in such allowances under this section, have been applied.

"(d) If the amount of the change in any educational assistance or subsistence allowance under subsection (a) is not a multiple of $0.10 it shall be raised to the next higher multiple of $0.10 in the case of a multiple of $0.05 or adjusted to the nearest multiple of $0.10 in any other case.

"(e) For purposes of this section—

"(1) the term 'price index' means the Consumer Price Index (all items, United States city average) published monthly by the Bureau of Labor Statistics; and the average level of the price index for the three months in any calendar quarter shall be deemed to be the level of the price index in such quarter; and

"(2) the term 'base period' means—

"(A) the calendar quarter commencing July 1, 1974, with respect to the first change under subsection (a); and

"(B) the calendar quarter immediately preceding the quarter in which the determination constituting the basis of the most recent change under subsection (a) was made, with respect to any change under subsection (a) after the first such change."

(b) The table of sections at the beginning of chapter 36 of title 38, United States Code, is amended by adding at the end thereof the following:

"1796. Cost-of-living changes in educational assistance and subsistence allowances."

(c) The amendment made by subsection (a) of this section shall apply only with respect to changes in educational assistance and subsistence allowances under chapters 31, 34, and 35 of title 38, United States Code, for months in and after the second calendar quarter beginning after the date of the enactment of this section on the basis of determinations made (under section 1796 of such title, as added by subsection (a) of this section) in and after the first calendar quarter beginning after the date of the enactment of this section.

NATIONAL COMMISSION ON SUPPLIES AND SHORTAGES ACT OF 1974—AMENDMENTS

AMENDMENTS NOS. 1441 AND 1442

(Ordered to be printed, and to lie on the table.)

Mr. HUMPHREY submitted two amendments, intended to be proposed by him, to the bill (S. 3523) to establish a Temporary National Commission on Supplies and Shortages.

ADDITIONAL COSPONSORS OF AMENDMENTS

AMENDMENT NO. 1348

At the request of Mr. HUMPHREY, the Senator from Indiana (Mr. HARTKE), the Senator from Maine (Mr. HATHAWAY), the Senator from Iowa (Mr. HUGHES), the Senator from Wyoming (Mr. MCGEE), the Senator from New Hampshire (Mr. MCINTYRE), the Senator from Minnesota (Mr. MONDALE), and the Senator from Wisconsin (Mr. NELSON) were added as cosponsors of Amendment No. 1348 to the bill (S. 2005) to provide adequate reserves of certain agricultural commodities, and for other commodities.

AMENDMENT NO. 1426

At the request of Mr. PROXMIRE, the Senator from Tennessee (Mr. BROCK) was added as a cosponsor of Amendment No. 1426 to the bill (H.R. 11221) to provide full deposit insurance for public units and to increase deposit insurance from $20,000 to $50,000.

NOTICE OF JOINT LEGISLATIVE HEARINGS ON PRIVACY AND GOVERNMENT INFORMATION SYSTEMS

Mr. ERVIN. Mr. President, hearings on bills relating to privacy and Government information systems will be held before an ad hoc subcommittee of the Senate Government Operations Committee and the Judiciary Subcommittee on Constitutional Rights on June 18, 19, and 20. The joint hearings will be held in room 3302 of the Dirksen Senate Office Building at 10 a.m.

The legislation before the Government Operations Committee is S. 3418, which I have cosponsored with Senators PERCY and MUSKIE, to establish an administrative structure to oversee rules for the gathering and disclosure of information concerning individuals, and to provide management systems in Federal agencies, State and local governments and other organizations concerning such information, and for other purposes.

Bills pending before the Constitutional Rights Subcommittee of which I am also chairman, are: S. 2810, introduced by Senator GOLDWATER, to protect the constitutional right of privacy of individuals concerning whom identifying numbers or identifiable information is recorded by enacting principles of information practice in furtherance of amendments I, III, IV, V, IX, X, and XIV of the U.S. Constitution;

S. 2542, introduced by Senator BAYH to protect the constitutional right of privacy of those individuals concerning whom certain records are maintained; and

S. 3116, introduced by Senator HATFIELD, to protect the individual's right to privacy by prohibiting the sale or distribution of certain information.

With these legislative hearings, the Government Operations Committee will continue its oversight of the development and uses of automatic data processing in the Federal Government. The intergovernmental nature of nationwide systems involving electronic and manual transmission, sharing and distribution of data about citizens has significant implications for our federal system. In its attempt to respond to citizens' demands for quality and quantity in services, government and the private sector have turned to the large data banks, computerized information systems and management techniques which will help them get the job done. Where these practices and systems neglect the administrative and technical concern for privacy, due process, and surveillance over the individual, they are taking a toll, which is yet unmeasured, on constitutional principles of accountability, responsibility and limited government. The cost to the taxpayer in dollars and cents concerns every American, for in the interest of promoting efficient government, the taxpayer may also be paying for loss of his privacy. That may be the price of insufficient monitoring by the public and Congress of the haphazard, ad hoc, ways modern government has found to meet its information needs, and which public officials use to meet their political needs.

Two Subcommittees of the Government Operations Committee are presently conducting oversight into major aspects of this problem. For instance, the Permanent Subcommittee on Investigations, chaired by Senator JACKSON, is presently conducting an inquiry into surveillance practices in and out of government, including government wiretapping, eavesdropping, recording, industrial espionage and bugging of labor negotiations, and other monitoring practices.

The Intergovernment Relations Subcommittee chaired by Senator MUSKIE, who is also a sponsor of the pending bill, is considering legislation concerning electronic surveillance and the need to reorganize departments and agencies engaging in such practices. That subcommittee is also studying a major aspect of Federal administration which affects individual privacy; this is the classification of Federal records and the laws and rules governing access, release and withholding of information which government collects about people.

The sponsors have introduced S. 3418 for purposes of discussion on the issues of what standards Congress should set for the protection of privacy in the development and management of Federal information systems, especially those which have been computerized with capacity for the sharing of records among departments and governments and across State boundaries. I expect

Mr. JAVITS. I point out that the list of States not covered includes such sparsely populated States as Montana and Louisiana, which happen to be the States of the majority leader and the chairman, as well as Hawaii, Idaho, Arkansas, North Dakota, and so forth. I thank the Senator from Utah for making that clear. There is no exclusivity about this.

Mr. LONG. Mr. President, I ask unanimous consent to have printed in the RECORD a list of the States that would benefit under what we were able to work out with the House.

There being no objection, the list was ordered to be printed in the RECORD, as follows:

States	Estimated maximum number of beneficiaries	Estimated maximum total additional costs (thousands)
Alaska	1,100–1,500	$600–$800
Maine	7,000–8,000	3,000–3,500
Massachusetts	49,300	30,000
Michigan	71,400–97,300	40,700–55,400
Nevada	6,700	3,600
New Jersey	80,000–120,000	48,000–72,000
Puerto Rico	33,000–42,000	9,000–11,000
Rhode Island	8,000–9,000	5,000
Vermont	3,600	2,000–3,000
Washington	42,000	17,000
Total	300,000–380,000	160,900–202,100
Federal share		80,000–101,000

The PRESIDING OFFICER. The question is on agreeing to the conference report.

The conference report was agreed to.

Mr. LONG. Mr. President, I move to reconsider the vote by which the conference report was agreed to.

Mr. BENNETT. I move to lay that motion on the table.

The motion to lay on the table was agreed to.

Mr. JAVITS. Mr. President, that commitment was given to myself and the Senator from California (Mr. TUNNEY) in October of 1972. Since that time, it has become clear that remedial action must be taken in order to permit the Federal-State extended unemployment compensation program to function as Congress intended. That need is highlighted by the string of temporary amendments to which Congress agreed in an attempt to remedy the defects in the trigger mechanism on a temporary basis in June 1973, December 1973, and March 1974.

These amendments will again lapse on July 1 of this year unless further action is taken. It is time that we sought a permanent solution to the inadequacy of those trigger requirements so that we can offer some measure of assurance to those workers who are unemployed that there will be an adequate program of benefits available to them.

The amendment that I am privileged to cosponsor would provide for the extended benefits program to trigger on in any State in which the insured unemployment rate equaled or exceeded 4 percent for any 13-week period. The off trigger would be activated when the insured unemployment rate in that State dropped below 4 percent for any 13-week period. The thrust of this amendment is to eliminate the requirement that the insured unemployment rate exceed the rate for the corresponding period of the previous 2 years by at least 20 percent. If any State is experiencing a severe unemployment problem, it is of little relevance, particularly to the individual unemployed worker seeking a job, whether that State has experienced such similar periods of high unemployment previously.

Under this amendment the following 24 States are currently eligible to pay extended unemployment benefits:

Alaska, California, Connecticut, Delaware, Hawaii, Idaho, Maine, Massachusetts, Michigan, Minnesota, Montana, Nevada, New Jersey, New Mexico, New York, North Dakota, Oregon, Pennsylvania, Puerto Rico, Rhode Island, Utah, Vermont, Washington, and West Virginia.

Only two States, Michigan and Delaware, would be eligible to continue paying those benefits after July 1 if this amendment is not agreed to. The continuation of this amendment would provide for the payment of extended benefits for up to 1,400,000 workers either currently receiving, or potentially eligible to receive benefits during ficsal year 1975.

I hasten to point out to the Senators that this amendment simply permits the States to trigger into the extended benefits program. It is still left to the discretion of the various States as to whether or not they wish to participate in the program. In addition, this amendment involves no increased general fund expenditures on the part of the Federal Government since the extended benefits program is financed in equal part from the various State unemployment accounts, and from the Federal extended benefits account, both of which are financed by an employer payroll tax.

Mr. President, I ask unanimous consent that a table showing the number of potential beneficiaries of this amendment supplied by the Department of Labor be inserted into the RECORD.

The PRESIDING OFFICER. Without objection, it is so ordered.

ESTIMATED EXTENDED BENEFITS, FISCAL YEAR 1975

[Assumptions: (1) Drop 120 percent Trigger Criteria; (2) Insured unemployment rate—3.8 percent; (3) All States affected will pass conforming legislation]

	Number of beneficiaries	Total costs (millions)
Alabama		
Alaska	2,000	$1.1
Arizona		
Arkansas	2,800	1.4
California	244,100	136.2
Colorado		
Connecticut	75,000	52.4
Delaware		
District of Columbia		
Florida		
Georgia		
Guam		
Hawaii	3,000	2.1
Idaho	3,100	1.0
Illinois		
Indiana		
Iowa		
Kansas		
Kentucky		
Louisiana		
Maine	19,200	7.0
Maryland		
Massachusetts	122,500	79.6
Michigan	143,200	85.9
Minnesota	12,500	4.9
Mississippi		
Missouri	15,000	$5.7
Montana	2,500	.7
Nebraska		
Nevada	7,800	4.5
New Hampshire		
New Jersey	167,400	101.0
New Mexico	2,900	.9
New York	270,000	164.7
North Carolina		
North Dakota	1,600	.6
Ohio		
Oklahoma		
Oregon	21,400	10.9
Pennsylvania	55,600	35.0
Puerto Rico	106,400	26.8
Rhode Island	21,200	12.0
South Carolina		
South Dakota		
Tennessee		
Texas		
Utah	1,500	.5
Vermont	4,700	3.0
Virginia		
Virgin Islands		
Washington	108,800	60.7
West Virginia	3,700	1.4
Wisconsin		
Wyoming		
United States total	1,417,900	800.0

Note: Costs would be shared 50–50 by States and Federal Government.

FAIR CREDIT BILLING ACT—AMENDMENT

AMENDMENT NO. 1438

(Ordered to be printed, and to lie on the table.)

Mr. PROXMIRE (for himself and Mr. BROCK) submitted an amendment, intended to be proposed by them, jointly, to the bill (H.R. 11221) to provide full deposit insurance for public units and to increase deposit insurance from $20,000 to $50,000.

INCREASE OF ALLOWANCES TO VETERANS—AMENDMENT

AMENDMENT NO. 1440

(Ordered to be printed, and to lie on the table.)

Mr. BELLMON. Mr. President, S. 2784 has recently been reported out of the Senate Veterans' Affairs Committee and placed on the Senate calendar. During consideration of this most important measure it is my intent to offer an amendment calling for an escalator subsistence and educational allowances similar to present provisions of the social security programs.

Mr. President, I ask unanimous consent that the full text of my amendment be printed in the RECORD at this point.

There being no objection, the amendment was ordered to be printed in the RECORD, as follows:

AMENDMENT NO. 1440

On page 105, line —, insert the following new section:

Title VI. Sec. 601. Chapter 36 of title 38, United States Code, is amended by adding at the end thereof a new section as follows:

"§ 1796. COST-OF-LIVING INCREASE IN EDUCATIONAL ASSISTANCE AND SUBSISTENCE ALLOWANCES.

"(a) As soon as possible after the beginning of each calendar quarter, the Administrator shall determine the extent by which the price index in the preceding calendar quarter was different than the price index

hearings to produce expert advice not only on the standards to be set, but on the scope of the bill and how far the law should affect State, local, and private data banks. The hearings will also help us determine what kind of Federal structure should be established to enforce or advise on standards.

Congress is now considering a number of legislative proposals directed to specific problem areas of the law governing the privacy of the individual such as criminal justice data banks, military surveillance of civilian politics, wiretapping and eavesdropping, private credit data banks, employee privacy, behavior modification, lie detectors, and computer technology. These are some of the techniques and governmental programs which have concerned Congress and the public.

In contrast to such special legislation, the proposals considered in the June hearings represent general legislation to protect the privacy of all citizens and to build into the structure and practices of government a strengthened respect for the privacy and other freedoms guaranteed by the Bill of Rights.

S. 3418 is similar, but not identical, to omnibus legislation introduced by Representatives EDWARD KOCH and BARRY GOLDWATER, JR., which is being considered by the House Government Operations Subcommittee on Foreign Operations and Government Information chaired by Representative WILLIAM MOORHEAD. Their joint efforts are contributing greatly to the chances for enactment of major privacy protections this year. Individually, many Members of the House of Representatives have for a number of years sponsored bills reflecting sections of this proposal relating to mailing lists, a Federal privacy board, Federal questionnaires, and changes in the freedom of information law.

Portions of S. 3418 are similar to the measures pending before the Constitutional Rights Subcommittee. Another portion is comparable to my bill S. 1791 of the 91st Congress, which was to limit the threats to privacy from burdensome, overly personal questionnaires by which Government agencies sought statistical information through coercive collection techniques.

S. 3418 and the related bills deal with requirements to reveal one's social security number to government and private organizations, with personal statistical questionnaires, mailing lists, and remedies for official information programs which may pass constitutional boundaries.

In addition to the thousands of complaints which people have sent to Congress, we now have for guidance on this subject the investigative hearings, reports, and findings of a number of congressional committees, private organizations and Government departments. One of these studies, "Records, Computers and Rights of Citizens," was ordered by the former Secretary of Health, Education, and Welfare, Elliot Richardson, who will testify on June 18 on the findings of his study and the need for congressional and administrative action.

Another influential and comprehensive report entitled "Privacy and Freedom" by the Association of the Bar of the City of New York was directed by Prof. Alan F. Westin of Columbia University. Recently, Dr. Westin conducted another study with Michael F. Baker for the National Academy of Sciences entitled "Databanks in a Free Society." I am pleased to announce that in addition to presenting testimony on the pending legislation, Dr. Westin has agreed to serve as a consultant to our hearings and to give us the benefits of his considerable research and analysis in this area of the law.

With the establishment of the new Domestic Council Committee on Right to Privacy chaired by the Vice President, Congress now has additional resources and assistance in its efforts to protect privacy, and we look forward to their cooperation in our studies.

Vice President FORD has accepted an invitation to present a statement on June 19 which will be delivered by the committee's Executive Director, Mr. Philip Buchan.

Other witnesses with special knowledge in this area of the law and administration will include Members of Congress who have sponsored privacy legislation, representatives of the National Governors Conference, the National Legislative Conference, the National Association for State Information Systems, Government Management Information Sciences, the National League of Cities, the U.S. Conference of Mayors, the American Civil Liberties Union, Liberty Lobby, public administration specialists, and other interested organizations and individuals.

The Subcommittee on Constitutional Rights conducted excellent hearings in March of this year on criminal justice data bank legislation, in 1971 on "Federal Data Banks, Computers and the Bill of Rights," and in 1969 on "Privacy, the Census and Federal Questionnaires." These hearings elicited for Congress a wealth of information about public complaints and attitudes concerning the establishment and the management of Federal programs to investigate citizens in order to store, distribute, and exchange information about them. We found that some of these programs were none of the business of the Government and infringed totally or in part on constitutional freedoms. Other programs were meant to obtain the great amount of information which Congress must have to legislate wisely and which the executive branch must have in order to administer the laws properly. In some instances, however, it was charged that lawful programs went beyond their purpose in scope, and in some cases, that the lack of adequate control permitted unauthorized access to this Government information, or allowed its transfer and distribution to unauthorized persons and those who had no need for it in the performance of their duties.

It is a rare person who has escaped the quest of modern government for information. Complaints which have come to the Constitutional Rights Subcommittee and to Congress over the course of several administrations show that this is a bipartisan issue which effects people in all walks of life. The complaints have shown that despite our reverence for the constitutional principles of limited Government and freedom of the individual, Government is in danger of tilting the scales against those concepts by means of its information-gathering tactics and its technical capacity to store and distribute information. When this quite natural tendency of Government to acquire and keep and share information about citizens is enhanced by computer technology and when it is subjected to the unrestrained motives of countless political administrators, the resulting threat to individual privacy make it necessary for Congress to reaffirm the principle of limited Government on behalf of freedom.

The complaints show that many Americans are more concerned than ever before about what might be in their records because Government has abused, and may abuse, its power to investigate and store information.

They are concerned about the transfer of information from data bank to data bank and black list to black list because they have seen instances of it.

They are concerned about intrusive statistical questionnaires backed by the sanctions of criminal law or the threat of it because they have been subject to these practices over a number of years.

The pending legislation represents a partial solution to these concerns. There are alternatives to some of the provisions. For instance, enforcement of the act and the advisory functions which are located in an independent privacy board might be relocated or distributed to the General Accounting Office and the courts. Furthermore, after receiving testimony the committee may want to alter the scope of the legislation.

I want to commend Senator PERCY for his interest in this subject and his initiative in working with House sponsors to bring the legislation before the Government Operations Committee in connection with its oversight of the use of governmental data banks and computer technology, and its monitoring of surveillance practices throughout government which may threaten freedom.

I hope the joint efforts of the Senate Government Operations Committee and the Constitutional Rights Subcommittee, whose members and staff have great expertise in this area of the law, will result in enactment of the basic legislative guarantees which are needed if America is to face up to the computer age.

It should be noted that these pending bills follow patterns and raise issues similar to those in criminal justice legislation, S. 2963 and S. 2964, which I have cosponsored with the following Senators who include members of the Judiciary and Government Operations Committees: Senators HRUSKA, MATHIAS, KENNEDY, BAYH, TUNNEY, YOUNG, BROOKE, MANSFIELD, ROBERT BYRD, BURDICK, ROTH, HUGH SCOTT, THURMOND, FONG, and GURNEY.

We welcome suggestions and comments from Members of Congress and

others with an interest in and knowledge about these matters. Those wishing to submit statements for the record should communicate with the Government Operations Committee, room 3306 of the Dirksen Office Building, Washington, D. C. 20510, telephone 225–7469.

In an article entitled "The First Amendment—A Living Thought in the Computer Age," from volume 4 of the Columbia Human Rights Review, 1972, I have described some of the many complaints which people have registered to the Constitutional Rights Subcommittee and to Members of Congress about attitudes and program of government which threaten the privacy guaranteed under the first amendment. At the conclusion of the article, there is suggested a seven-part legislative program to remedy these complaints, part of which is reflected in the pending legislation. Additional examples of questionable data banks have been revealed, many of them documented in the forthcoming report of the subcommittee's comprehensive survey of the laws and rules affecting individual privacy in Federal data banks and computerized information systems. These new revelations to Congress merely serve to reaffirm my conviction that early congressional action is needed to implement the Constitution.

I ask unanimous consent that the articles be printed at this point in the RECORD.

There being no objection, the articles were ordered to be printed in the RECORD, as follows:

[From the Columbia Human Rights Review, Volume 4, No. 1 (1972)]

THE FIRST AMENDMENT: A LIVING THOUGHT IN THE COMPUTER AGE[1]

(By SAM J. ERVIN, Jr.*)

Sherwood Anderson wrote words about America as true today as they were in the third decade of this century:

"America ain't cemented and plastered yet. They're still building it. . . . All America asks is to look at it and listen to it and understand it if you can. Only the understanding ain't important either; the important thing is to believe in it even if you don't understand it, and then try to tell it, put it down. Because tomorrow America is going to be something different, something more and new to watch and listen to and try to understand; and, even if you can't understand, believe."

Anyone seeking to understand contemporary America must deal with our national experience with computer technology. They must understand that it has become an essential tool in the "cementing and plastering" of our nation. They must understand that it has at once presented our country its greatest hope and its greatest challenge; keeping faith with our historical heritage and commitment to freedom, while enjoying the fruits of a rich industrialized society under a democratic constitution.

Throughout our nation the people involved with computer technology have charge of a great national resource which will affect the course of our economic and social progress. More important, insofar as it affects the exercise of governmental power and the power of large special interest groups, the new technology may help determine the course of freedom and human rights in our land.

In the process, I believe Americans could find wisdom in Sherwood Anderson's advice "to believe" in America. I say this because, as we grasp for the new computer technology and seek theories of systems analysis for our social problems, Americans may tend to forget to look to their own history. Some, in their haste to solve today's problems, may fear to translate America's promise of freedom into the program language of the computer age.

Those whose are initiated into the technological mysteries of computer hardware and software may take great pride. Through their deeds and genius they have helped people go to the moon, produce music, create art, conduct off-track betting, run railroads, and administer welfare systems. They help maintain our national defense and they keep our economy running. They aid in catching criminals and they establish instant credit. They locate marriage-mates for people and they prejudge elections almost before the votes are cast.

A tape storage system has been described which will make it possible to store a dossier on every living person in the United States and to retrieve any one of them in a maximum of 28 seconds. With such feats to their credit, these people know better than anybody that in the application of their knowledge, they plan a major role in the economic and social well-being of our society. They are responsible for bringing to our nation all the wondrous blessing of computer technology, especially scientific methods of processing information.

They can bend these machines to their will and make them perform feats undreamed of ten or even five years ago.

They have a special understanding of the new information flow charts for the vast data systems in our government.

They hold the access code to control over the technology as it affects the individual in our society.

They may hold the key to the final achievement of the rule of law which is the promise of our constitution.

With this body of knowledge, therefore, they bear special responsibility for the preservation of liberty in our country. That they have accepted this responsibility is clear from the *Privacy* themes of many recent conferences of computer professionals, equipment manufacturers, and computer users in the governmental and private sectors.

Their power is not limited to their technical expertise, but is augmented by the sheer numbers in the computer-related professions.

Advertisements on TV, radio, in newspapers, and even on buses daily remind the public of the inducements and rewards of a career in computer and data processing fields.

In the Federal Government, their numbers are growing. An inventory of automatic data processing equipment shows that in 1952 there were probably two computers in government. In 1971, there were 5,961.[2]

In 1960, there were 48,700 man-years used in federal automated data processing functions. This includes systems analysis and design, programming, equipment selection and operation, key punching, equipment maintenance and administrative support. In 1970, there were about 136,504 man-years used in direct ADP work.

A recent illuminating report by the National Association for State Information Systems shows that in 35 states in 1971, over twenty-four and a half thousand people were engaged in ADP. Twenty-eight states together spent 181 million dollars of their budgets on such personnel.[3]

To glance through their professional journals, newspapers and bulletins each month is to be constantly amazed at the breadth and reach of the theories and accomplishments.[4] It also deepens a layman's wonder at the complex language which sometimes defies translation into ordinary English.

For all of these reasons, the general public stands in superstitious awe of the skills and knowledge, the machines and instruments, and the products derived and transmitted by them. For the uninitiated, the computer print-out bears a mystique and an aura of scientific rationality which makes it appear infallible. This is true for most lawyers and probably for most people in political life.

There is a theory abroad today in academic circles that America is divided into two worlds. One of them is the world of science and technology,[5] inhabited by people who are part of a technological and electronic revolution. In the other world are said to live all the rest of the people whose ideas and values are based on an earlier age.

In accordance with their theory, some have tried to stamp the scientist with motives and values different from those of other Americans; with goals oriented only toward efficiency or shorn of compassion, or, alternatively, with exclusive ability to determine social priorities. I cannot agree with this analysis, for I believe there is a yearning in every human heart for liberty, and for the freedom to express oneself according to the dictates of conscience. Despite a man's commitment to a chosen profession, he wants the freedom to fulfill himself as an individual and to use his God-given faculties free from the coercion of government.

So I do not believe Americans dwell in two worlds. Regardless of our origins, I believe we share a common heritage and a common destiny in that we are all engaged in seaching for freedom. We share, according to the mandates of the Constitution, a common understanding that the best protection for that freedom rests on the limitations on the power of government and on the division of that power.

I cannot agree with such an analysis for another reason. Since the Senate Constitutional Rights Subcommittee began its study of computers, data banks and the Bill of Rights, I have received many letters from computer specialists, systems designers, engineers, programmers, professors and others in the scientific community which prove that despite, and perhaps because of their professions, they share the same concern about invasion of privacy as all other Americans, the same apprehensions about excesses of governmental surveillance and inquiries. Above all, they realize, perhaps better than others, that while the information technology they deal with can extend the intellect of man for the betterment of society, it also extends the power of government a millionfold.[6]

It makes it possible for government to administer more efficiently and to offer vastly better services to the taxpayers.

At the same time, it extends and unifies official power to make inquiries, conduct investigations, and to take note of the thoughts, habits and behavior of individuals. Of course, government has always had such power, but on a much smaller scale than today. Similarly, men possessing the power of government have always had the capacity for bad motives, simple errors or misguided purpose. There have always been problems with errors in the manual files. Now, computers may broadcast the image of these errors throughtout a national information system.

What the electronic revolution has done is to magnify any adverse affects flowing from these influences on the life of the individual and on his proper enjoyment of the rights, benefits and privileges due a free man in a free society.

I reject the notion of division of Americans on the basis of scientific and technological values. If I had the unhappy and well-nigh impossible task of distinguishing two types of Americans, I believe I would distinguish between those who understand the

Footnotes at end of article.

terized dossiers. It also illustrates the lack of sufficient criminal, civil, or administrative sanctions against unwarranted sharing and disclosure of such confidential information. To my knowledge, no punitive action was taken except for a disciplinary personnel action filed against an agent of the Federal Bureau of Investigation, who was then allowed to retire.

The weakness of any applicable regulations is demonstrated by the report of the Bureau of Narcotics and Dangerous Drugs that its current disclosure order "would not cover the release of collateral intelligence information, information contained in dead files, or information on nondefendants, such as that disclosed in the Alioto testimony." The Bureau further stated that under the provisions of its new Agents Manual it is only a "breach of integrity" to make unauthorized disclosure of files which are restricted to official use.[35]

MISUSE OF MILITARY INTELLIGENCE RECORDS

Another case [36] illustrates how the Army's investigative intelligence services and files were put to private use to obtain the dismissal of an employee of a private business. In this instance an Army intelligence agent whose routine duties involved security investigations and surveillance for the Army's civil disturbance prevention program described to the Subcommittee how he was ordered by his superiors to conduct an investigation of the bank loan records, police and court records of the private citizen and was told to give the resulting information to the employee's supervisor. He later learned that the investigation had been ordered by an intelligence officer as a personal favor for an official of the company. When the agent reported this to his superiors, he was told in a classified letter that the matter involved "national security." A year later, following his separation from the service, the agent reported the incident to the Inspector General of the Assistant Chief of Staff for the Pentagon, who began an investigation. All of his allegations were confirmed and firm disciplinary actions were taken against the guilty officers. It was too late, however, for the subject of the Army investigative report, who had already been dismissed.

These cases illustrate the concerns over political administrative and technical problems of access, confidentiality and purging of erroneous or outdated records in computer systems. But these are issues which have long concerned legislatures, bar associations and others.

The major reason for public apprehension about computer technology and information sciences is the use of them to acquire, process, analyze and store information about activities and matters which are protected by the First Amendment.

What people writing to Congress fear most is the uses to which this technology may be put by men of little understanding but great zeal. They know that, applied to unlawful or unwise programs, computers merely absorb the follies and foibles of misguided politically-minded administrators.

In Federal Government, the new technology, combined with extended Federal-state services and their spin-off information systems, have produced vast numbers of investigators, analysts, and programmers devoted to the study of people and society. With the zeal of dedicated civil servants, they are devoted to the building of data bases on the habits, attitudes and beliefs of law-abiding citizens. Much of what they gather is trivial; much of it goes far beyond the needs of government. Some of it is shared extensively and often unnecessarily by agencies who are components of these large information systems.

People seeking government jobs in some agencies are told to reply to personality tests asking:

I believe there is a God.

I believe in the second coming of Christ.

I believe in a life hereafter.

I am very religious (more than most people).

I go to church almost every week.

I am very strongly attracted by members of my own sex.

I love my father.

My sex life is satisfactory.

Once in a while I feel hate toward members of my family whom I usually love.

I wish I were not bothered by thoughts about sex.

When the Subcommittee held hearings on these practices, government officials explained that there was no right or wrong answer to the questions, that the responses were coded and analyzed by the computer.[37]

I asked whether they did not think such inquiries violated the privacy of the individual's thought about matters that were none of the business of government. The reply was that there was no Supreme Court decision holding that people who apply for federal employment have a constitutional right to privacy.

There was a Civil Service program telling employees to fill out computer punch cards stating their racial, ethnic or national origin along with their social security number.[38] In the land renowned for being the "melting pot" of the world, over 3 million individuals had to analyze their backgrounds and reduce them to one of four squares on an IBM card. If they protested that these matters were none of the business of government, they were blacklisted in their offices and harassed with computer-produced orders to return the completed questionnaire. The resemblances between this program and those of totalitarian governments in our recent history were all too obvious.

The Census Bureau makes more use of computer technology for personal inquiries than anyone.[39] It conducts surveys for its own uses backed by the criminal and civil sanctions. One of these, the decennial census, asked people such questions as:

Marital Status: Now married, divorced, widowed, separated, never married.

(If a woman) How many babies have you ever had, not counting stillbirths?

Do you have a flush toilet?

Have you been married more than once?

Did your first marriage end because of death of wife or husband?

What was your major activity 5 years ago?

What is your rent?

What is your monthly electric bill?

Did you work at any time last week?

Do you have a dishwasher? Built-in or portable?

How did you get to work last week? (Driver, private auto; passenger, private auto; subway; bus; taxi; walked only; other means).

How many bedrooms do you have?

Do you have a health condition or disability which limits the amount of work you can do at a job?

How long have you had this condition or disability?

Under even heavier sanctions, the Census Bureau puts questionnaires to farmers, lawyers, owners of businesses, and others, selected at random, about the way they handle their business and finances.[40]

The Census Bureau also makes surveys for many other departments and agencies.[41] For example, they put out statistical questionnaires which the Department of Health, Education, and Welfare wanted to send to retired people asking:

How often they call their parents;

What they spend on presents for grandchildren;

How many newspapers and magazines they buy a month;

If they wear artificial dentures;

"Taking things all together, would you say you're very happy, pretty happy, or not too happy these days?"

And many other questions about things on which government has no business demanding answers.

These people are not told that their answers are voluntary, but are harassed to reply and are given the impression they will be penalized if they do not answer.[42]

There are many other examples of inquiring social and economic data that are backed by the psychological, economic, or penal sanction of government. Clearly, Government has great need for all kinds of information about people in order to govern efficiently and administer the laws well; similarly, Congress must have large amounts of meaningful information in order to legislate wisely.

However, I believe these examples of governmental data collection illustrate my contention that the First Amendment wraps up the principle of free speech, which includes the right to speak one's thoughts and opinions as well as the right to be free of governmental coercion to speak them.

There are other examples of government programs which, well-meaning in purpose, are fraught with danger for the very freedoms which were designed to make the minds and spirits of all Americans free, and which work to keep America a free society. A number of these would be impractical, if not impossible, without the assistance of computer technology and scientific data processing.

It is those First Amendment freedoms which are the most precious rights conferred upon us by our Constitution: the freedom to assemble peaceably with others and petition government for a redress of grievances; the freedom to worship according to the dictates of one's own conscience free of government note-taking; the freedom to think one's own thoughts regardless of whether they are pleasing to government or not; the freedom to speak what one believes whether his speech is pleasing to the government or not; the freedom to associate with others of like mind to further ideas or policies which one believes beneficial to our country, whether such association is pleasing to government or not.

THE SECRET SERVICE

In the pursuit of its programs to protect high government officials from harm and federal buildings from damage,[43] the Secret Service has been pressured to create a computerized data bank. Their guidelines for inclusion of citizens in this data bank requested much legitimate information but also called for information on "professional gate crashers;" "civil disturbances;" "anti-American or anti-U.S. Government demonstrations in the United States or overseas;" pertaining to a threat, plan, or attempt by an individual or group to "embarrass persons protected by the Secret Service or any other high U.S. Government official at home or abroad;" "persons who insist upon personally contacting high government officials for the purpose of redress of imaginary grievances;" and "information on any person who makes oral or written statements about high government officials in the following categories: (1) threatening statements, (2) irrational statements, and (3) abusive statements."

Americans have always been proud of their First Amendment freedoms which enable them to speak their minds about the shortcomings of their elected officials. As one in political life, I have myself received letters I considered abusive. Similarly, I have uttered words which others have deemed abusive. While I am not a "professional gate crasher," I am a malcontent on many issues. I have written the President and other high government officials complaining of grievances which some may consider imaginary; and on occasion, I may also have "embarrassed" high government officials.

One man wrote me his concern about this program and commented:

Footnotes at end of article.

"The Secret Service ought to go after my mother-in-law, too. On her last visit she said that the Vice President doesn't seem to have too many brains. She also said that Senator —— has a face like a carbuncle. Should I report this to the Secret Service? [44]

There is no doubt that the physical protection of the President and high government officials is a legitimate government purpose and all reasonable means must be taken in pursuit of it. Nevertheless, such broad and vaguely worded standards for investigating and adversely reporting Americans to their government on the basis of their utterances could, at one time or another, include most members of Congress and most politically aware citizens. It could cover heated words exchanged in political debate and discussion anywhere in the country. Yet civil and military officials throughout the Federal government and in some local law enforcement agencies were requested to report people coming to their attention who were thought to fit these criteria.

The Subcommittee has not received complete answers to our questionnaire on the subject of this computer and the national reporting system it serves. However, we have indications that other broad and zealous information programs, including the Army civil disturbance system,[45] are sharing or feeding on entries which, if not carefully evaluated, may produce serious consequences for the rights and privileges of citizens. Illustrating the misunderstandings and misinterpretations possible is the fact that military doctors have expressed to me their concern about an allegedly "secret" agreement between the Defense Department and the Secret Service which they were told was a recent one and which required reporting of all servicemen receiving administrative discharges. One psychiatrist writes of his concern for the confidentiality of medical records in such action:

"I see very little reason for this. My impression of the individuals whom I recommended for such a discharge was that these were immature individuals who were not able to adapt to the service for one reason or another. Not by any stretch of the imagination were these individuals unpatriotic or a threat to the security of the nation." [46]

When I asked the Secretary of the Navy about this, the Subcommittee was informed that a person is not reported to the Secret Service merely because he received an administrative discharge from the Navy or Marine Corps.[47] However, we were informed that Pursuant to Naval regulations issued under a secret 1965 Agreement,[48] the Navy reports an average of 400 persons annually. We learned, for example, that among the many categories of people to be reported were not only servicemen but civilian employees of the Defense Department who were discharged on security or suitability grounds and who showed "evidence of emotional instability or irrational or suicidal behavior, expressed strong or violent sentiments against the United States," or who had "previous arrests, convictions, conduct or statements indicating a propensity for violence and antipathy for good order in Government." [49]

MILITARY SPYING

Another example of First Amendment information programs is the Army program for spying on Americans who exercised their First Amendment rights. Despite these rights, and despite the constitutional division of power between the federal and state governments, despite laws and decisions defining the legal role and duties of the Army, the Army was given the power to create an information system of data banks and computer programs which threatened to erode these restrictions on governmental power.[50]

Allegedly, for the purpose of predicting and preventing civil disturbances which might develop beyond the control of state and local officials, Army agents were sent throughout the country to keep surveillance over the way the civilian population expressed their sentiments about government policies. In churches, on campuses, in classrooms, in public meetings, they took notes, tape-recorded, and photographed people who dissented in thought, word or deed. This included clergymen, editors, public officials, and anyone who sympathized with the dissenters.

With very few, if any, directives [51] to guide their activities, they monitored the membership and policies of peaceful organizations who were concerned with the war in Southeast Asia, the draft, racial and labor problems, and community welfare. Out of this surveillance the Army created blacklists of organizations and personalities which were circulated to many federal, state and local agencies, who were all requested to supplement the data provided. Not only descriptions of the contents of speeches and political comments were included, but irrelevant entries about personal finances, such as the fact that a militant leader's credit card was withdrawn. In some cases, a psychiatric diagnosis taken from Army or other medical records was included.

This information on individuals was programmed into at least four computers according to their political beliefs, or their memberships, or their geographic residence.[52]

The Army did not just collect and share this information. Analysts were assigned the task of evaluating and labeling these people on the basis of reports on their attitudes, remarks and activities. They were then coded for entry into computers or microfilm data banks.[53]

The Army attempts to justify its surveillance of civilians by asserting that it was collecting information to enable the President to predict when and where civilians might engage in domestic violence, and that the President was empowered to assign this task to it by the statutes conferring upon him the power to use the armed forces to suppress domestic violence.

I challenge the validity of this assertion.

Under our system, the power to investigate to determine whether civilians are about to violate federal laws is committed to federal civil agencies, such as the FBI; and the power to investigate to determine whether civilians are about to violate state laws is reposed in state law enforcement officers.

If President Johnson believed he ought to have had information to enable him to predict when and where civilians might engage in future domestic violence, he ought to have called upon the FBI or appropriate state law enforcement officers for the information.

He had no power to convert the Army into a detective force and require it to spy on civilians.

This conclusion is made plain by the Constitution and every act of Congress relating to the subject. Sections 331, 332, 333 and 334 of Title 10 of the United States Code certainly did not confer any such power on the President. These statutes merely authorized him to use the armed forces to suppress domestic violence of the high degree specified in them, and conditioned their use for that purpose upon his issuing a proclamation immediately ordering the offenders "to disperse and retire peaceably to their abodes within a limited time."

The only other statute relevant to the subject is section 1385 of Title 18 of the Code, which prohibits the use of any part of the Army or Air Force "as a posse comitatus or otherwise to execute the law . . . except in cases and under circumstances expressly authorized by the Constitution or Act of Congress."

The legislative history of this statute is fully revealed in the opinion of United States District Judge Dooling in *Wrynn v. United States,* 200 F. Supp. 457 (E.D.N.Y. 1961). When the words of this statute are read in the light of its legislative history, it is obvious that the statute is not limited by the expression "as a posse comitatus or otherwise," but operates as a prohibition against the use of the Army to execute the laws without reference to whether it is employed as a posse comitatus or as a portion of the Army. Indeed, the statute embodies "the inherited antipathy of the American to the use of troops for civil purposes." [200 F. Supp. at 465].

President Johnson's use of the troops to spy on civilians, to build data banks and create computerized information systems, discloses that relevance of this statute to our day is sadly clear. Since neither the Constitution nor any Act of Congress expressly, or impliedly, authorized such use, the President was forbidden by section 1385 of Title 18 of the United States Code to use the Army to spy on civilians.

The Army's spying violated First Amendment freedoms of the civilians who became aware that they or the groups to which they belonged had been placed under surveillance. This is so because it undoubtedly stifled their willingness to exercise their freedom of speech, association and assembly.[54]

If any proof were needed of the logic and truth of this statement, it can be drawn from such testimony as the Subcommittee received from Dr. Jerome Wiesner who commented:

"Many, many students are afraid to participate in political activities of various kinds which might attract them because of their concern about the consequences of having a record of such activites in a central file. They fear that at some future date, it might possibly cost them a job or at least make their clearance for a job more difficult to obtain." [55]

The Subcommittee has heard no testimony yet that the Army's information program was useful to anyone. The only result of the testimony by the Defense Department was to confirm my belief that under the Constitution and under the laws, the Army had no business engaging in such data-gathering and that the scope and breadth of the surveillance was so broad as to be irrelevant to the purpose.

Congress has still to discover the complete truth about these Army computers. Apparently, even officials responsible for intelligence did not know of the existence of the computers for implementing the program. The Subcommittee has repeatedly requested the testimony of the Army Generals who would be most knowledgeable about the computers and what they contained. We have just as repeatedly been denied their testimony as well as delivery and declassification of pertinent documents demonstrating the scope and purpose of the program.[56] The Army said it would cut back on the data-gathering on lawabiding citizens and would defer to the Department of Justice. So I asked the Justice Department officials how many computers that Department had containing information on people who lawfully exercised their First Amendment freedoms." [57]

I had seen newspaper articles quoting the director of the Justice Department's Interdivisional Information Unit. He said there that the computer's list of thousands of names is not a register of "good guys" or "bad guys." "It is simply a list of who participated in demonstrations, rallies and the like." This would include non-violent people as well as violent, he said.[58] On the basis

Footnotes at end of article.

proper limits and uses of governmental power and those who do not.

However much we try to rationalize decisions through the use of machines, there is one factor for which the machine can never allow. That is the insatiable curiosity of government to know everything about those it governs. Nor can it predict the ingenuity applied by government officials to find out what they think they must know to achieve their ends.

It is this curiosity, combined with the technological and electronic means of satisfying it, which has recently intensified governmental surveillance and official inquiries that I believe infringe on the constitutional rights of individuals.

Congress received so many complaint about unauthorized government data banks and information programs that the Subcommittee undertook a survey to discover what computerized and mechanized data banks government agencies maintain on people, especially about their personal habits, attitudes, and political behavior. We have also sought to learn what government-wide or nation-wide information systems have been created by integrating or sharing the separate data bases. Through our questionnaire, we have sought to learn what laws and regulations govern the creation, access and use of the major data banks in government.[7]

The replies we are receiving are astounding, not only for the information they are disclosing, but for the attitudes displayed toward the right of Congress and the American people to know what Government is doing.

In some cases, the departments were willing to tell the Subcommittee what they were doing, but classified it so no one else could know.[8] In one case, they were willing to tell all, but classified the legal authority on which they relied for their information power.[9]

Some reports are evasive and misleading. Some agencies take the attitude that the information belongs to them and that the last person who should see it is the individual whom it is about.[10] A few departments and agencies effectively deny the information by not responding until urged to do so.[11]

They reflect the attitude of the Army captain who knew Congress was investigating the Army data banks and issued a directive stating:

"The Army General Counsel has re-emphasized the long-standing policy of the Executive Branch of the Government . . . that all files, records and information in the possession of the Executive Branch is privileged and is not releasable to any part of the Legislative Branch of the Government without specific direction of the President."[12]

So, on the basis of this study, and on the withholdings of information from the American people which the Subcommittee has experienced, [13] I have concluded that the claim of the Government departments to their own privacy is greatly overstated. The truth is that they have too much privacy in some of their information activities. They may cite the Freedom of Information Act [14] as authority for keeping files secret from the individual as well as from the Congress. They then turn around and cite "inherent power"[15] or "housekeeping authority"[16] as a reason for maintaining data banks and computerized files on certain individuals; or they may cite the conclusions of independent Presidential factfinding commissions.[17]

So far the survey results show a very wide-ranging use of such technology to process and store the information and to exchange it with other federal agencies, with state and local governments and, sometimes, with private agencies.

Most of this is done in connection with administration of Government's service programs. However, a number of these data banks and information programs may partake of the nature of largescale blacklists. This is so because they may encompass masses of irrelevant, outdated or even incorrect investigative information based on personalities, behavior and beliefs. Unwisely applied or loosely supervised, they can operate to deprive a person of some basic right.

For instance, a Federal Communications Commission response [18] shows that the FCC uses computers to aid it in keeping track of political broadcast time, in monitoring and assigning spectrums, and in helping it make prompt checks on people who apply for licenses. The Commission reported that it also maintains a Check List, which now has about 10,900 names. This Check List, in the form of a computer print-out, is circulated to the various Bureaus within the Commission. It contains the names and addresses of organizations and individuals whose qualifications are believed to require close examination in the event they apply for a license. A name may be put on the list by Commission personnel for a variety of reasons, such as a refusal to pay an outstanding forfeiture, unlicensed operation, license suspension, the issuance of a bad check to the Commission or stopping payment on a fee check after failing a Commission examination.

In addition, this list incorporates the names and addresses of individuals and organizations appearing in several lists prepared by the Department of Justice, other Government agencies, and Congressional committees. For example, the list contains information from the "FBI Withhold List," which contains the names of individuals or organizations which are allegedly subversive, and from the Department of Justice's "Organized Crime and Racketeering List," which contains the names of individuals who are or have been subjects of investigation in connection with activities identified with organized crime. Also included in the list are names obtained from other Government sources, such as the Internal Revenue Service, the Central Intelligence Agency, and the House Committee on Internal Security. According to the Commission, the use of the data arose in 1964 because during the course of Senate Hearings chaired by Senator McClellan, it was discovered that a reputed racketeering boss in New Orleans, Louisiana, held a Commission license. In order that such licensing not take place in the future, the Commission established liaison with the responsible divisions within the Department of Justice to be kept current on persons who might have such affiliations.

The Civil Service Commission maintains a "security file" in electrically powered rotary cabinets containing 2,120,000 index cards.[19] According to the Commission, these bear lead information relating to possible questions of suitability involving loyalty and subversive activity. The lead information contained in these files has been developed from published hearings of Congressional committees, State legislative committees, public investigative bodies, reports of investigation, publications of subversive organizations, and various other newspapers and periodicals. This file is not new, but has been growing since World War II.

The Commission chairman reported:

"Investigative and intelligence officials of the various departments and agencies of the Federal Government make extensive official use of the file through their requests for searches relating to investigations they are conducting."

In another "security investigations index" the Commission maintains 10,250,000 index cards filed alphabetically covering personnel investigations made by the Civil Service Commission and other agencies since 1939. Records in this index relate to incumbents of Federal positions, former employees, and applicants on whom investigations were made or are in process of being made.

Then, the Commission keeps an "investigative file" of approximately 625,000 file folders containing reports of investigation on cases investigated by the Commission. In addition, about 2,100,000 earlier investigative files are maintained at the Washington National Records Center in security storage. These are kept to avoid duplication of investigations or for updating previous investigations.

The Housing and Urban Development Department in considering automation of a departmental system which would integrate records now included in FHA's Sponsor Identification File, Department of Justice's Organized Crime and Rackets File, and HUD's Adverse Information File[20] A data bank consisting of approximately 325,000 3 x 5 index cards has been prepared covering any individual or firm which was subject of or mentioned prominently in, any investigations dating from 1954 to the present. This includes all FBI investigations of housing matters as well.

In the area of law enforcement, the Bureau of Customs has installed a central automated data processing intelligence network which is a comprehensive data bank of suspect information available on a 24-hour-a-day basis to Customs terminals throughout the country.[21]

According to the Secretary of the Treasury:

"These records include current information from our informer, fugitive and suspect lists that have been maintained throughout the Bureau's history as an enforcement tool and which have been available at all major ports of entry, though in much less accessible and unable form. With the coordinated efforts of the Agency Service's intelligence activities, steady growth of the suspect files is expected."

There is the "Lookout File" of the Passport Office and the Bureau of Security and Consular Affairs.[22] This computerized file illustrates the "good neighbor" policy agencies observe by exchanging information in order to keep individuals under surveillance for intelligence and law enforcement purposes. Maintained apart from the twenty million other passport files, its basic purpose is to assist in screening passport applicants to make certain they are citizens of the United States and that they are eligible to receive passports. Requests for entry into this system are received from component agencies of the Department, from other government agencies, or in the limited category of child custory, from an interested parent or guardian.

The Department assured the Subcommittee that data recorded in this "Lookout File" is not disseminated. Rather, it serves as a "flag" which, if a "hit" or suspect is recorded, is furnished to the original source of the lookout and consists of the name of the individual and the fact that he has applied for a passport. The individual is not told that he is in the file until the information is used adversely against him. Then, according to the report, "he is fully informed and given an opportunity to explain or rebut the information on which the adverse action is based."

Among some of the reasons listed for people being in the Lookout File are the following:

If the individual's actions do not reflect to the credit of U.S. abroad;

If he is wanted by a law enforcement agency in connection with criminal activity;

If a court order restricting travel is outstanding or the individual is involved in a custody or desertion case;

"If he is a known or suspected Communist or subversive;

"If he is on the Organized Crime and Rackets List or is a suspected delinquent in military obligations."

Footnotes at end of article.

The Defense Industrial Security Clearance Office is preparing to computerize its card files on over one and a half million private citizens who are employees of businesses doing classified contract work for the Federal Government.[23]

The Federal Deposit Insurance Corporation maintains information on people now associated with banks insured by the FDIC or who have been associated with such banks in the past.[24] It keeps a file on the names of individuals gained from newspapers and other public sources if they are characterized as having an unsatisfactory relationship with any insured bank or any closed insured bank. This also includes information supplied to the Corporation by other investigative or regulatory agencies on persons connected with an insured bank.

The Army maintains the U.S. Army Investigative Records Repository (USAIRR) which contains about 7,000,000 files relating principally to security and criminal investigations of former and present members of the Army, civilian employees and employees of private contractors doing business with the Army. The other services maintain similar investigative files.[25]

There is a Defense Central Index of Investigation operated by the Army for the entire Defense Department. The Index is designed to locate any security or criminal investigative file for any Defense agency and will be computerized shortly. It contains identifying data such as name, date of birth and social security number on people who have ever been the subject of investigations.[26]

There are all the data banks and computers in the Department of Justice [27] for intelligence, for civil disturbance prevention; for "bad checks passers;" for organized crime surveillance; and for federal-state law enforcement cooperation through the computerized National Crime Information Center.

On the basis of our investigation of complaints reviewed by Congress,[28] I am convinced that people throughout the country are more fearful than ever before about those applications of computer technology and scientific information processing which may adversely affect their constitutional rights. Furthermore, my study of the Constitution convinces me that their fears are well founded.

First, they are concerned that through a computer error they may be denied basic fairness and due process of law with respect to benefits and privileges for which they have applied.

Secondly, they are concerned about illegal access and violation of confidentiality of personal information which is obtained about them by government or industry.

These are actions which for any one individual or for entire groups may lead to a loss of the ability to exercise that "pursuit of happiness" which the Declaration of Independence declares is one of the unalienable rights of man.

These are actions which, by producing erroneous reports, may limit or deny a person's economic prospects and thereby impair that liberty which under the 5th and 14th amendments government may not impair without due process of law.

ARREST RECORDS

This possibility is illustrated by a letter [29] I received from a man who describes the effect on his life of an incident which occurred when he was fifteen years of age. In connection with a locker theft, he was taken to the police station, finger-printed, questioned and then he left, cleared of charges. He was not involved in any incident subsequently except a few minor traffic violations. He served 11 years in the armed services and held the highest security clearances. After gaining employment with a city government, he discovered that the youthful incident was, 15 years later, part of an FBI file and distributed to employers on request. He was asked to explain the incident for personnel records and to state why he withheld the information. Although he was unaware of the record, he believes the failure to list the incident was a factor in not gaining employment in several instances, and he was told he would have to institute court action to have the record expunged.

The problem he and millions of others face with respect to their records is illustrated by a regulation issued by the Attorney General last year restating the goal of the Federal Bureau of Investigation "to conduct the acquisition, collection, exchange, classification, and preservation of identification records . . . on a mutually beneficial basis." [30] Among the agencies listed as eligible to receive and supply information were railroad police, banking institutions and insurance companies.

In Washington, D.C., a young man who was an innocent bystander during a campus demonstration was arrested by police and then released. Knowing that the FBI could distribute such records to employers, he hired a lawyer and spent large sums of money in a suit to have his arrest record expunged. The lower court denied his request, but the Court of Appeals ruled that, in the District of Columbia at least, arrest records should be expunged for innocent bystanders caught up in mass police arrests.[31]

In another case, a young man was arrested on probable cause and fingerprinted in California. When the police could not connect him with the case, he was released. He sought to have his arrest record expunged, or alternatively, to have strict limitations placed on its dissemination to prospective employers and others by the Federal Bureau of Investigation. While the U.S. District Court denied his request for expungement, it did say that his arrest record may not be revealed to prospective employers except in the case of any Federal agency when he seeks employment with that agency. However, it could be distributed for law enforcement purposes. Congress later restored this power to the FBI temporarily in an annual appropriation bill.

Judge Gesell's comments in this case of *Menard* v. *Mitchell* [32] are significant for the issue of arrest records, but also for the Army's computer surveillance program and for many other government intelligence systems now being designed. He stated that while "conduct against the state may properly subject an individual to limitations upon his future freedom within tolerant limits, accusations not proven, charges made without supporting evidence when tested by the judicial process, ancient or juvenile transgressions long since expiated by responsible conduct, should not be indiscriminately broadcast under governmental auspices." He also said:

"The increasing complexity of our society and technological advances which facilitate massive accumulation and ready regurgitation of farflung data have presented more problems in this area, certainly problems not contemplated by the framers of the Constitution. These developments emphasize a pressing need to preserve and to redefine aspects of the right of privacy to insure the basic freedoms guaranteed by this democracy.

"A heavy burden is placed on all branches of Government to maintain a proper equilibrium between the acquisition of information and the necessity to safeguard privacy. Systematic recordation and dissemination of information about individual citizens in a form of surveillance and control which may easily inhibit freedom to speak, to work, and to move about in this land. If information available to Government is misused to publicize past incidents in the lives of its citizens the pressures for conformity will be irresistible. Initiative and individuality can be suffocated and a resulting dullness of mind and conduct will become the norm. We are far from having reached this condition today, but surely history teaches that inroads are most likely to occur during unsettled times like these where fear or the passions of the moment can lead to excesses."

There are many similar cases pending throughout the states. Present laws are not sufficient to assure that an individual will be judged on his merit and not by inacurrate arrests records distributed by a national law enforcement computer.[33]

LAW ENFORCEMENT INTELLIGENCE RECORDS

Such threats to privacy and liberty arise with special force in the area of intelligence records. The Subcommittee study reveals two serious problems which have acquired national urgency through the introduction of computer technology. First, the problem of safeguarding intelligence information from improper release by government itself, and secondly, the problem of confining its collection to appropriate areas and subjects.

Government has, and should have, power to collect information, even raw, univerified intelligence information, in fields in which government has a lawful, legitimate interest. But this great power imposes a solemn responsibility to see that no one is given access to that information, except the Government itself for some legitimate purpose. There could never, for instance, be justification for Government to disclose intelligence gathered about citizens pursuant to its powers, to other citizens for their own personal or financial aggrandizement. Nor should Government through disclosure of confidential documents aid and abet the writing of sensational articles in private journals operated for commercial profit.

Nevertheless, the Subcommittee received testimony and evidence about two cases, which illustrate the misuse of confidential intelligence information for such purposes.

One involved a man in political life, the mayor of San Francisco, who was the subject of an article in Look Magazine purporting to establish that he associated with persons involved in organized crime. When the Mayor sued the magazine for libel, he undertook through subpoena power to learn the basis for such charges and where and how the authors obtained their information. He learned that they had received confidential information and documents from intelligence data banks. The information came from files and computer printouts of a number of major Federal, state and local government law enforcement agencies. They involved the U.S. Attorney General's Office, the Federal Bureau of Investigation, Internal Revenue Service, Federal Bureau of Narcotics, the Customs Bureau, the Immigration and Naturalization Service, the California Criminal Identification and Investigation Bureau, the California State Department of Justice, and the Intelligence Unit of the Los Angeles Police Department. By their own testimony for the case, the authors of the article admitted that they examined, obtained or borrowed originals or copies of such law enforcement records containing much raw unevaluated intelligence information on numerous people including the names of three U.S. Presidents, the state Governor, a number of Senators, and many private law-abiding citizens, not accused of any crime. These documents were obtainable despite the fact that many of them were stamped "Confidential" or—

Property of U.S. Government For official use only. May not be disseminated or contents disclosed without permission. . . ."

There is more about these and other disclosures in the hearing record but I believe the Mayor's testimony [34] illustrates many of the dangers to privacy in this age of large investigative networks and instant compu-

Footnotes at end of article.

proper limits and uses of governmental power and those who do not.

However much we try to rationalize decisions through the use of machines, there is one factor for which the machine can never allow. That is the insatiable curiosity of government to know everything about those it governs. Nor can it predict the ingenuity applied by government officials to find out what they think they must know to achieve their ends.

It is this curiosity, combined with the technological and electronic means of satisfying it, which has recently intensified governmental surveillance and official inquiries that I believe infringe on the constitutional rights of individuals.

Congress received so many complaint about unauthorized government data banks and information programs that the Subcommittee undertook a survey to discover what computerized and mechanized data banks government agencies maintain on people, especially about their personal habits, attitudes, and political behavior. We have also sought to learn what government-wide or nation-wide information systems have been created by integrating or sharing the separate data bases. Through our questionnaire, we have sought to learn what laws and regulations govern the creation, access and use of the major data banks in government.[7]

The replies we are receiving are astounding, not only for the information they are disclosing, but for the attitudes displayed toward the right of Congress and the American people to know what Government is doing.

In some cases, the departments were willing to tell the Subcommittee what they were doing, but classified it so no one else could know.[8] In one case, they were willing to tell all, but classified the legal authority on which they relied for their information power.[9]

Some reports are evasive and misleading. Some agencies take the attitude that the information belongs to them and that the last person who should see it is the individual whom it is about.[10] A few departments and agencies effectively deny the information by not responding until urged to do so.[11]

They reflect the attitude of the Army captain who knew Congress was investigating the Army data banks and issued a directive stating:

"The Army General Counsel has re-emphasized the long-standing policy of the Executive Branch of the Government . . . that all files, records and information in the possession of the Executive Branch is privileged and is not releasable to any part of the Legislative Branch of the Government without specific direction of the President."[12]

So, on the basis of this study, and on the withholdings of information from the American people which the Subcommittee has experienced, [13] I have concluded that the claim of the Government departments to their own privacy is greatly overstated. The truth is that they have too much privacy in some of their information activities. They may cite the Freedom of Information Act [14] as authority for keeping files secret from the individual as well as from the Congress. They then turn around and cite "inherent power"[15] or "housekeeping authority"[16] as a reason for maintaining data banks and computerized files on certain individuals; or they may cite the conclusions of independent Presidential factfinding commissions.[17]

So far the survey results show a very wide-ranging use of such technology to process and store the information and to exchange it with other federal agencies, with state and local governments and, sometimes, with private agencies.

Most of this is done in connection with administration of Government's service programs. However, a number of these data banks and information programs may partake of the nature of largescale blacklists. This is so because they may encompass masses of irrelevant, outdated or even incorrect investigative information based on personalities, behavior and beliefs. Unwisely applied or loosely supervised, they can operate to deprive a person of some basic right.

For instance, a Federal Communications Commission response [18] shows that the FCC uses computers to aid it in keeping track of political broadcast time, in monitoring and assigning spectrums, and in helping it make prompt checks on people who apply for licenses. The Commission reported that it also maintains a Check List, which now has about 10,900 names. This Check List, in the form of a computer print-out, is circulated to the various Bureaus within the Commission. It contains the names and addresses of organizations and individuals whose qualifications are believed to require close examination in the event they apply for a license. A name may be put on the list by Commission personnel for a variety of reasons, such as a refusal to pay an outstanding forfeiture, unlicensed operation, license suspension, the issuance of a bad check to the Commission or stopping payment on a fee check after failing a Commission examination.

In addition, this list incorporates the names and addresses of individuals and organizations appearing in several lists prepared by the Department of Justice, other Government agencies, and Congressional committees. For example, the list contains information from the "FBI Withhold List," which contains the names of individuals or organizations which are allegedly subversive, and from the Department of Justice's "Organized Crime and Racketeering List," which contains the names of individuals who are or have been subjects of investigation in connection with activities identified with organized crime. Also included in the list are names obtained from other Government sources, such as the Internal Revenue Service, the Central Intelligence Agency, and the House Committee on Internal Security. According to the Commission, the use of the data arose in 1964 because during the course of Senate Hearings chaired by Senator McClellan, it was discovered that a reputed racketeering boss in New Orleans, Louisiana, held a Commission license. In order that such licensing not take place in the future, the Commission established liaison with the responsible divisions within the Department of Justice to be kept current on persons who might have such affiliations.

The Civil Service Commission maintains a "security file" in electrically powered rotary cabinets containing 2,120,000 index cards.[19] According to the Commission, these bear lead information relating to possible questions of suitability involving loyalty and subversive activity. The lead information contained in these files has been developed from published hearings of Congressional committees, State legislative committees, public investigative bodies, reports of investigation, publications of subversive organizations, and various other newspapers and periodicals. This file is not new, but has been growing since World War II.

The Commission chairman reported:

"Investigative and intelligence officials of the various departments and agencies of the Federal Government make extensive official use of the file through their requests for searches relating to investigations they are conducting."

In another "security investigations index" the Commission maintains 10,250,000 index cards filed alphabetically covering personnel investigations made by the Civil Service Commission and other agencies since 1939. Records in this index relate to incumbents of Federal positions, former employees, and applicants on whom investigations were made or are in process of being made.

Then, the Commission keeps an "investigative file" of approximately 625,000 file folders containing reports of investigation on cases investigated by the Commission. In addition, about 2,100,000 earlier investigative files are maintained at the Washington National Records Center in security storage. These are kept to avoid duplication of investigations or for updating previous investigations.

The Housing and Urban Development Department in considering automation of a departmental system which would integrate records now included in FHA's Sponsor Identification File, Department of Justice's Organized Crime and Rackets File, and HUD's Adverse Information File[20] A data bank consisting of approximately 325,000 3 x 5 index cards has been prepared covering any individual or firm which was subject of or mentioned prominently in, any investigations dating from 1954 to the present. This includes all FBI investigations of housing matters as well.

In the area of law enforcement, the Bureau of Customs has installed a central automated data processing intelligence network which is a comprehensive data bank of suspect information available on a 24-hour-a-day basis to Customs terminals throughout the country.[21]

According to the Secretary of the Treasury:

"These records include current information from our informer, fugitive and suspect lists that have been maintained throughout the Bureau's history as an enforcement tool and which have been available at all major ports of entry, though in much less accessible and unable form. With the coordinated efforts of the Agency Service's intelligence activities, steady growth of the suspect files is expected."

There is the "Lookout File" of the Passport Office and the Bureau of Security and Consular Affairs.[22] This computerized file illustrates the "good neighbor" policy agencies observe by exchanging information in order to keep individuals under surveillance for intelligence and law enforcement purposes. Maintained apart from the twenty million other passport files, its basic purpose is to assist in screening passport applicants to make certain they are citizens of the United States and that they are eligible to receive passports. Requests for entry into this system are received from component agencies of the Department, from other government agencies, or in the limited category of child custory, from an interested parent or guardian.

The Department assured the Subcommittee that data recorded in this "Lookout File" is not disseminated. Rather, it serves as a "flag" which, if a "hit" or suspect is recorded, is furnished to the original source of the lookout and consists of the name of the individual and the fact that he has applied for a passport. The individual is not told that he is in the file until the information is used adversely against him. Then, according to the report, "he is fully informed and given an opportunity to explain or rebut the information on which the adverse action is based."

Among some of the reasons listed for people being in the Lookout File are the following:

If the individual's actions do not reflect to the credit of U.S. abroad;

If he is wanted by a law enforcement agency in connection with criminal activity;

If a court order restricting travel is outstanding or the individual is involved in a custody or desertion case;

"If he is a known or suspected Communist or subversive;

"If he is on the Organized Crime and Rackets List or is a suspected delinquent in military obligations."

Footnotes at end of article.

asking:

Footnotes at end of article.

If they wear artificial dentures;

"Taking things all together, would you say you're very happy, pretty happy, or not too happy these days?"

ances which some may consider imaginary; and on occasion, I may also have "embarrassed" high government officials.

One man wrote me his concern about this program and commented:

The Defense Industrial Security Clearance Office is preparing to computerize its card files on over one and a half million private

highest security clearances. After gaining employment with a city government, he discovered that the youthful incident was 15

the pressures for conformity will be irresistible. Initiative and individuality can be suffo-

"The Secret Service ought to go after my mother-in-law, too. On her last visit she said that the Vice President doesn't seem to have too many brains. She also said that Senator —— has a face like a carbuncle. Should I report this to the Secret Service? [44]

There is no doubt that the physical protection of the President and high government officials is a legitimate government purpose and all reasonable means must be taken in pursuit of it. Nevertheless, such broad and vaguely worded standards for investigating and adversely reporting Americans to their government on the basis of their utterances could, at one time or another, include most members of Congress and most politically aware citizens. It could cover heated words exchanged in political debate and discussion anywhere in the country. Yet civil and military officials throughout the Federal government and in some local law enforcement agencies were requested to report people coming to their attention who were thought to fit these criteria.

The Subcommittee has not received complete answers to our questionnaire on the subject of this computer and the national reporting system it serves. However, we have indications that other broad and zealous information programs, including the Army civil disturbance system,[45] are sharing or feeding on entries which, if not carefully evaluated, may produce serious consequences for the rights and privileges of citizens. Illustrating the misunderstandings and misinterpretations possible is the fact that military doctors have expressed to me their concern about an allegedly "secret" agreement between the Defense Department and the Secret Service which they were told was a recent one and which required reporting of all servicemen receiving administrative discharges. One psychiatrist writes of his concern for the confidentiality of medical records in such action:

"I see very little reason for this. My impression of the individuals whom I recommended for such a discharge was that these were immature individuals who were not able to adapt to the service for one reason or another. Not by any stretch of the imagination were these individuals unpatriotic or a threat to the security of the nation." [46]

When I asked the Secretary of the Navy about this, the Subcommittee was informed that a person is not reported to the Secret Service merely because he received an administrative discharge from the Navy or Marine Corps.[47] However, we were informed that Pursuant to Naval regulations issued under a secret 1965 Agreement,[48] the Navy reports an average of 400 persons annually. We learned, for example, that among the many categories of people to be reported were not only servicemen but civilian employees of the Defense Department who were discharged on security or suitability grounds and who showed "evidence of emotional instability or irrational or suicidal behavior, expressed strong or violent sentiments against the United States," or who had "previous arrests, convictions, conduct or statements indicating a propensity for violence and antipathy for good order in Government." [49]

MILITARY SPYING

Another example of First Amendment information programs is the Army program for spying on Americans who exercised their First Amendment rights. Despite these rights, and despite the constitutional division of power between the federal and state governments, despite laws and decisions defining the legal role and duties of the Army, the Army was given the power to create an information system of data banks and computer programs which threatened to erode these restrictions on governmental power.[50]

Allegedly, for the purpose of predicting and preventing civil disturbances which might develop beyond the control of state and local officials, Army agents were sent throughout the country to keep surveillance over the way the civilian population expressed their sentiments about government policies. In churches, on campuses, in classrooms, in public meetings, they took notes, tape-recorded, and photographed people who dissented in thought, word or deed. This included clergymen, editors, public officials, and anyone who sympathized with the dissenters.

With very few, if any, directives [51] to guide their activities, they monitored the membership and policies of peaceful organizations who were concerned with the war in Southeast Asia, the draft, racial and labor problems, and community welfare. Out of this surveillance the Army created blacklists of organizations and personalities which were circulated to many federal, state and local agencies, who were all requested to supplement the data provided. Not only descriptions of the contents of speeches and political comments were included, but irrelevant entries about personal finances, such as the fact that a militant leader's credit card was withdrawn. In some cases, a psychiatric diagnosis taken from Army or other medical records was included.

This information on individuals was programmed into at least four computers according to their political beliefs, or their memberships, or their geographic residence.[52]

The Army did not just collect and share this information. Analysts were assigned the task of evaluating and labeling these people on the basis of reports on their attitudes, remarks and activities. They were then coded for entry into computers or microfilm data banks.[53]

The Army attempts to justify its surveillance of civilians by asserting that it was collecting information to enable the President to predict when and where civilians might engage in domestic violence, and that the President was empowered to assign this task to it by the statutes conferring upon him the power to use the armed forces to suppress domestic violence.

I challenge the validity of this assertion.

Under our system, the power to investigate to determine whether civilians are about to violate federal laws is committed to federal civil agencies, such as the FBI; and the power to investigate to determine whether civilians are about to violate state laws is reposed in state law enforcement officers.

If President Johnson believed he ought to have had information to enable him to predict when and where civilians might engage in future domestic violence, he ought to have called upon the FBI or appropriate state law enforcement officers for the information.

He had no power to convert the Army into a detective force and require it to spy on civilians.

This conclusion is made plain by the Constitution and every act of Congress relating to the subject. Sections 331, 332, 333 and 334 of Title 10 of the United States Code certainly did not confer any such power on the President. These statutes merely authorized him to use the armed forces to suppress domestic violence of the high degree specified in them, and conditioned their use for that purpose upon his issuing a proclamation immediately ordering the offenders "to disperse and retire peaceably to their abodes within a limited time."

The only other statute relevant to the subject is section 1385 of Title 18 of the Code, which prohibits the use of any part of the Army or Air Force "as a posse comitatus or otherwise to execute the law . . . except in cases and under circumstances expressly authorized by the Constitution or Act of Congress."

The legislative history of this statute is fully revealed in the opinion of United States District Judge Dooling in *Wrynn v. United States*, 200 F. Supp. 457 (E.D.N.Y. 1961). When the words of this statute are read in the light of its legislative history, it is obvious that the statute is not limited by the expression "as a posse comitatus or otherwise," but operates as a prohibition against the use of the Army to execute the laws without reference to whether it is employed as a posse comitatus or as a portion of the Army. Indeed, the statute embodies "the inherited antipathy of the American to the use of troops for civil purposes." [200 F. Supp. at 465].

President Johnson's use of the troops to spy on civilians, to build data banks and create computerized information systems, discloses that relevance of this statute to our day is sadly clear. Since neither the Constitution nor any Act of Congress expressly, or impliedly, authorized such use, the President was forbidden by section 1385 of Title 18 of the United States Code to use the Army to spy on civilians.

The Army's spying violated First Amendment freedoms of the civilians who became aware that they or the groups to which they belonged had been placed under surveillance. This is so because it undoubtedly stifled their willingness to exercise their freedom of speech, association and assembly.[54]

If any proof were needed of the logic and truth of this statement, it can be drawn from such testimony as the Subcommittee received from Dr. Jerome Wiesner who commented:

"Many, many students are afraid to participate in political activities of various kinds which might attract them because of their concern about the consequences of having a record of such activites in a central file. They fear that at some future date, it might possibly cost them a job or at least make their clearance for a job more difficult to obtain." [55]

The Subcommittee has heard no testimony yet that the Army's information program was useful to anyone. The only result of the testimony by the Defense Department was to confirm my belief that under the Constitution and under the laws, the Army had no business engaging in such data-gathering and that the scope and breadth of the surveillance was so broad as to be irrelevant to the purpose.

Congress has still to discover the complete truth about these Army computers. Apparently, even officials responsible for intelligence did not know of the existence of the computers for implementing the program. The Subcommittee has repeatedly requested the testimony of the Army Generals who would be most knowledgeable about the computers and what they contained. We have just as repeatedly been denied their testimony as well as delivery and declassification of pertinent documents demonstrating the scope and purpose of the program.[56] The Army said it would cut back on the data-gathering on lawabiding citizens and would defer to the Department of Justice. So I asked the Justice Department officials how many computers that Department had containing information on people who lawfully exercised their First Amendment freedoms." [57]

I had seen newspaper articles quoting the director of the Justice Department's Interdivisional Information Unit. He said there that the computer's list of thousands of names is not a register of "good guys" or "bad guys." "It is simply a list of who participated in demonstrations, rallies and the like." This would include non-violent people as well as violent, he said.[58] On the basis

Footnotes at end of article.

of these reports, I asked for the testimony of this official, but for some strange reason, he could not be located.

Despite questioning during the hearings and correspondence with the Justice Department, we have been unable to obtain an accurate description of the use of Justice Department computers for collecting, processing and analyzing information on lawful First Amendment activities of citizens. Nor have we been able to ascertain or obtain the standards followed by the Department in deciding what individuals should be the subjects in such files, or how they should be excluded from such files.

LEGISLATIVE REMEDIES

There has been much discussion of the need for new laws granting access to individual records. I believe a person should have the chance to expunge, update and correct his records. With the advent of systematic record-keeping, a man needs the chance which a businessman has to go into economic bankruptcy and obtain a discharge from his past.

I believe, however, that we must go beyond that relationship between the individual and his records. We must act to restore a healthy balance to the relationship between the citizen and his government, and necessarily between Congress and the Executive Branch. Mere access to and knowledge of his individual file is not enough. Remedial action must be addressed to the curbing of the power of government over the individual and to restricting its power to deny information about government programs. The claim to an inherent power to monitor, investigate and compile dossiers on law-abiding citizens on the off-chance that they might need to be investigated for a legitimate governmental purpose at some time in the future must also be opposed.

As a result of the Subcommittee's experience in playing hide-and-go-seek with the Federal Government's computers and with the people who plan and supervise them, I am convinced these computers have too much privacy today. The Congress, the press and the public should have available an *habeas corpus* action for entire computer systems and programs themselves. No department should be able to hide such broad-based data programs and information systems. If they are lawful, the American people then have a right to full knowledge about the operation of their government. If they are not lawful and relevant for some purpose, they should be exposed for what they are—attempts to intimidate citizens into silence and conformity.

First, we need to devise some judicial remedy for confronting and testing the nature, purpose, legality and constitutionality of governmental data banks and large-scale intelligence information systems which by their very existence may threaten the quality of our First Amendment freedoms or whose contents may affect economic prospects, reputations or rights. Now pending before the United States Supreme Court is just such a challenge to the Army surveillance program and the military data banks, including at least four computer systems for storing and processing information on American across the land. [*Tatum v. Laird*, no. 71–288 (1971) (argued March 27, 1972)] The lower court has denied standing to sue to plaintiffs who were subjects of surveillance and computer dossiers on grounds that they have not shown injury. [444 F.2d 947 (D.C. Cir. 1971)].

Congress must strengthen and enforce reporting requirements for computer systems. Not even in the audit of computers which the present law requires the General Services Administration to conduct each year is it possible for Congress, the press, and the public to get minimum information about all of the management uses of computers in government.

Secondly, I believe we must devise legal means of assuring the reporting of large government data banks to a central office established independently of the executive branch. This would require the filing of policy statements describing exactly what agencies feed a particular information system and who would receive or access data routinely from a particular data bank. These policy statements should be public records. In this way, people would have due notice of possible sharing of information by other agencies or state or local governments.

Thirdly, out of these directives, a graphic national information-flow chart would be designed and made available for public inspection. An individual concerned about his record could then go to the respective agencies and exercise his rights under the Freedom of Information Law to inspect his files.

Fourth, there is a need to fully implement the principle of open government implicit in the Freedom of Information Law by reducing the number of exemptions in it which the Executive Branch may use to deny or withhold information. This would make the judicial remedies it contains more meaningful.

Fifth, I believe there must be established a new independent agency for setting and enforcing strict standards in software and hardware for the assurance of security, confidentiality and privacy of records. These would be applied to all phases of gathering, processing and transmitting information about people by government computer systems. This would include such problems as interception of electronic transmissions and tapping of systems.

Sixth, Congress must enact specific prohibitions on unconstitutional or unwise practices which unfairly augment government's power to invade individual privacy. Examples of such legislation would be: (1) a ban on use of military resources to conduct unwarranted surveillance over civilians and to create and share data banks on them, and (2) a ban on unconstitutional means of coercing citizens into revealing personal information about themselves.[59] Such a bill is S. 2156 which would prohibit requirements on applicants and employees to submit to lie detectors in order to work.[60] Another bill is S. 1438, designed to protect federal employees and applicants from unwarranted demands for information about such matters as their race, national origin, religious beliefs and practices, sexual attitudes and conduct, and personal family relationships.[61] Another necessary protection would be a prohibition on distribution of arrest records to private companies and severe restrictions on their availability within government.[62]

Seventh, is the need for America to take a stand on whether or not every person is to be numbered from cradle to grave, and if so whether or not that number is to be the social security number. Until now, the idea of a universal standard identifier has been merely discussed in philosophical terms, but the need to reduce people to digits for the computer age has prompted wide government use of the number for identifying individuals in government files. Private industries, businesses and organizations have followed suit to the dismay of many people who have registered strong complaints against this practice with the Subcommittee. They were supported by the findings of a Social Security Task Force which reported in 1971 that:

"The increasing universality of the Social Security Number in computer data collection and exchange presents both substantial benefits and potential dangers to society; and that in order to maximize the benefits and minimize the dangers, there needs to be developed a national policy on computer data exchange and personal identification in America, including a consideration of what safeguards are needed to protect individuals' rights of privacy and due process."[63]

In outlining the areas in which state legislatures and the Congress must make important judgments, this Task Force stated:

"Defining the proper role of the Social Security Number in society requires that broad social judgments be made first about the desirability of large-scale computer record-keeping in various settings; second, about the kinds of data necessary and appropriate to record about individuals within a given setting; third, about the safeguards needed to insure that the computer is being used within a given setting in ways that protect fundamental human rights; and fourth, about the desirability of *any* kind of universal identification system in terms of its psychological impact on the individual citizen."[64]

SUMMARY

From the Subcommittee study of privacy and government data banks one conclusion is undeniable. This is that the extensive use of computerized systems to classify and analyze men's thoughts, speech, attitudes, and lawful First Amendment behavior raises serious questions of denial of substantive due process to our entire society. To try to condense the truth about what men believe and why they believe is a futile exercise which can lead to that tyranny over the mind against which Thomas Jefferson swore eternal hostility. Without grave dangers to our constitutional system, we cannot permit government to reduce the realities of our political life and the healthy traffic in our marketplace of ideas to marks on magnetic tapes and data on a microfilm.

Professor Robert Boguslaw[65] eloquently described the dangers posed by this "technology-screened power" when he wrote that "the specification of future and current system states within this orientation characteristically requires an insistence upon a uniformity of perspective, a standardization of language, and a consensus of values that is characteristic of highly authoritarian social structures. Nonconforming perspectives, language, and values can be and, indeed, must be excluded as system elements."

He further points out certain engineering truths and certain human truths which face every politician, administrator, analyst and programmer who tries to use computers to convey either more or less than the straight facts about people. First is the truth that the strength of high-speed computers is precisely in their capacity to process binary choice data rapidly. But to process these data, the world of reality must at some point in time be reduced to binary form. Second is the truth "that the range of possibilities is ultimately set by the circuitry of the computer, which places finite limits on alternatives for data storage and processing." Third is the truth "that the structure of the language used to communicate with the computer restricts alternatives." Then there is the truth "that the programmer himself, through the specific sets of data he uses in his solution to a programming problem and the specific techniques he uses for his solution, places a final set of restrictions on action alternatives available within a computer-based system."

It is in this sense that computer programmers, the designers of computer equipment, and the developers of computer languages possess power in our society.

These limitations of men as well as machines are what I remembered as I listened to the young Army analyst describing his assignment to condense truth for the Army data systems by assigning numbers to people on the basis of their speech and thoughts.[66]

On the shoulders of technology experts who are aware citizens rests the responsibility for guiding those politicians who seek computer-based solutions to political prob-

Footnotes at end of article.

lems. At this point in our history, they, more than anyone, realize that computers have only those values which are designed and programmed into them.

If the attitude of the present Administration is any indication, Government will make increasing use of computer technology in pursuit of its current claim to an inherent power to investigate lawful activities and to label people on the basis of their thoughts. Municipal, state and federal agencies continue to plan, devise and build intelligence systems for many purposes. It devolves on those people involved in computer technology to make known the restrictions and the limitations of the machines as well as the alternatives for what is proposed. When the political managers ignore or abdicate their responsibility to assure the application of due process of law, they may have the final say over the constitutional uses of power.

What they say may not be popular with those who use their services, especially government departments. But I would suggest that when they advise on extending the power of government, they serve a higher law—the Constitution.

The technological forces which affect the quality of our freedoms come in many guises and under strange terminology. They are dreamers who would decry the advent of the computer as casting some sorcerer's shadow across an idyllic land. In their philosophical rejection or fear of this most intricate of machines, they would deny the spark of divinity which is the genius of man's mind; they would reject the progress of civilization itself. So there is no reason to condemn out of hand every governmental application of computers to the field of information processing or to systems study.

Our society has much to gain from computer technology. To assure against its political misuse, however, we need new laws restricting the power of government and implementing constitutional guarantees. We need increased political awareness of an independent nature by information specialists who understand the machines and the systems they constitute.

We do not, as some suggest, need new constitutional amendments to deal with these problems. The words of the original amendments will do, because they envelop our national concepts of personal freedom and I believe they can encompass anything which jeopardizes that freedom.

As Justice Oliver Wendell Holmes said:

"A word is not a crystal, transparent and unchanged; it is the skin of a living thought and may vary greatly in color and content according to the circumstances and the time in which it is used." [67]

I believe that Americans will have to work harder than ever before in our history so that the First Amendment remains a living thought in this computer age.

Otherwise, we may find the individual in our society represented not by a binary form, but by one digit.

And that will be "zero."

Otherwise, America may lose its cherished reputation as "the land of the Second Chance."

FOOTNOTES

* U.S. Senator, North Carolina.

[1] Based on an address before the Spring Joint Computer Conference of the Federation of Information Processing Societies, Atlantic City, N.J., May 20, 1971.

[2] INVENTORY OF AUTOMATED DATA PROCESSING EQUIPMENT IN THE UNITED STATES FISCAL YEAR 1971, GENERAL SERVICES ADMINISTRATION, at 15. A report providing information on the digital electronic computers installed throughout the U.S. Government, which defines "computer" as a configuration of EDPE components which includes one central processing system concept which recognizes the growing importance of configurations with more than one central processing unit. This report responds to requirements of P.L. No. 89-306, Stat. (Oct. 30, 1965) and S. Doc. No. 15 (1965), REPORT TO THE PRESIDENT ON THE MANAGEMENT OF AUTOMATIC DATA PROCESSING IN THE FEDERAL GOVERNMENT.

[3] 1970 NASIS REPORT, INFORMATION SYSTEMS TECHNOLOGY IN STATE GOVERNMENT at 18, developed by the State of Illinois and the National Association for State Information Systems, Council of State Governments.

[4] *See generally* COMPUTERWORLD (a weekly periodical servicing the computer community): DATAMATION: DATA MANAGEMENT; and BUSINESS AUTOMATION.

[5] *See, e.g.*, Brzezinksi, Between Two Ages, America's Role In the Technotronic Era, although all authors do not engage in such distinctions with the same judgments or purposes.

[6] *Hearings on Federal Data Banks, Computers and the Bill of Rights Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 92d Cong., 1st Sess. [Feb. 23-25 and Mar. 2-4, 9-11, 15 and 17 (1971)] [hereinafter cited as as *1971 Hearings*.] Testimony of Robert Bigelow, attorney, describing concern of professional computer organizations and press, *id.* at 680; Bibliography, lists of public discussions on privacy and computers in the United States and abroad, *id.* at 692 *et seq.*; Testimony of professor Caxton Foster, University of Mass., Department of Computer and Information Sciences, *id.* at 707.

[7] For a sample of questionnaire sent to all agencies and departments with slight alterations, see Letter to Secretary of Defense Melvin Laird, July 20, 1970 *1971 Hearings* at 1182, and to Attorney General Mitchell, June 9, 1970. *Id.* at 1212.

[8] *See, eg.*, State Department response to questionnaire, concerning its "Lookout File." *See* Letter of Sept. 9, 1970 to Subcommittee Chairman from Assistant Secretary of Defense Robert Moot, and list of classified enclosures, *1971 Hearings* at 1186.

[9] Navy Department response, Aug. 13, 1970, citing a Roosevelt Executive memorandum assigning responsibilities for intelligence activities. *Id.* at 1201.

[10] Department of Transportation response. Testimony of Secretary Volpe. *Id.* at 720. Many other agencies will inform the individual of the general contents of his file, if he is denied some right, benefit or privilege and regulations permit a hearing or right of confrontation or cross-examination—but not before.

[11] Department of Health, Education, and Welfare, series of letters over a two year period on file with Subcommittee, and as of March, 1972, no response has been received containing substantive answers.*

[12] Directive, ICGP-G-S3, Jan. 9, 1971, *Release of Official Information to Legislative Branch of Government. 1971 Hearings*, at 1179.

[13] Ervin, *Secrecy in a Free Society*, 213 NATION 454 (1971). *See generally Hearings on Executive Privilege Before the Subcomm. on Separation of Powers of the Senate Comm. on the Judiciary*, 92d Cong., 1st Sess. (1971). Testimony by Senator Tunney at 381 and William Rehnquist at 420.

[14] 5 U.S.C. § 552 (1970).

[15] *See, e.g., 1971 Hearings*, at 375, 431, 385. Testimony of Assistant Secretary of Defense Froehlke. *Id.* at 602, 599; testimony of Assistant Attorney General Rehnquist, note 13, *supra*.

[16] *See, e.g.*, Justice Department response to Subcommittee questionnaire.

[17] For Defense Department reliance on the findings of the National Advisory Commission on Civil Disorders (Kerner Commission), see testimony of Assistant Secretary of Defense Froehlke, *1971 Hearings*, at 379; noting the Commission's finding that the "absence of accurate information, both before and during disorder, has created special control problems for police," and the recommendation that "Federal-State planning should ensure that Federal troops are prepared to provide aid to cities. . . ."

The Department also cited a report filed by Cyrus Vance following the Detroit 1967 disturbances. *1971 Hearings*, at 378.

For law enforcement reliance on the Kerner Commission and similar commissions, *see e.g.*, testimony of Richard Velde for the *Law Enforcement Assistance Administration. 1971, Hearings* at 608:

Several States also developing with LEAA funds information systems related to civil disorders. Most of these systems have as their objective either tension detection and forecasting or providing support to tactical units. It should be noted that the Kerner Commission studied this problem carefully and recommended that the police develop adequate intelligence for tension-detecting as well as on-the-scene information for tactical units. Many of the systems LEAA supports in the civil disorders area arose out of the recommendations of the Kerner Commission and similar commissions established by the States.

For reliance on Warren Commission finding of information gaps, *see* response to Subcommittee questionnaires by the Secret Service, Nov. 21, 1969, reprinted at 115 CONG. REC. 39,114 (1969), and by the State Department Jan. 4 and Mar. 10, 1970; both responses in Subcommittee file.

[18] Response to questionnaire, in Subcommittee files, Mar. 25, 1971.

[19] *Id.* Aug. 18, 1970.

[20] *Id.* June 22, 1970.

[21] Id. May 28, 1970.

[22] *Id.* Jan. 4, 1970.

[23] *Id.* Aug. 1970. *See also 1971 Hearings*, at 375, Froehlke testimony on this and other Defense Department records systems.

[24] Response to questionnaire, Feb. 22, 1972. *See also* 12 U.S.C. § 1811 *et seq.* (1964), Amendments to Federal Deposit Insurance Act, requiring bank recording and reporting to Internal Revenue Service transactions, S. REP. 91-1139 and H.R. REP. 91-975.

[25] *See* note 23 *supra*.

[26] Response to Subcommittee questionnaire, Aug. 1970. Also described in Froehlke testimony, note 23, *supra* and in Army Undersecretary Beal letter of Mar. 20, 1970, reprinted in *1971 Hearings, Part II* at 1051, and at 116 CONG. REC. 26327-51 (1970).

[27] For descriptions and citations to supporting statutes and regulations, *see* response to Subcommittee questionnaires, *1971 Hearings, Part II* at 1312-68. *See also* discussion in testimony of Justice Department officials. *Id. Part I* at 597, 849.

[28] For descriptions and summaries of some of these complaints and concerns. Remarks of Senator Ervin, 116 CONG. REC. 30,-797, 41,751, 43,944 and 117 CONG. REC. S. 985 (daily ed. Feb. 8, 1971). In particular, note opening statements by Subcommittee Chairman each day of *1971 Hearings* outlining issues of concern for the day. Of interest here is a Dec. 1971 report, *A National Survey of the Public's Attitude Toward Computers*, sponsored by the American Federation of Information Processing Societies and TIME MAGAZINE noting that:

There is major concern about the use of large computerized information files. Thirty-eight percent of those surveyed believe computers represent a real threat to people's privacy as opposed to fifty-four percent who disagreed. Sixty-two percent are concerned that some large organizations keep information about millions of pepole. In addition, fifty-three percent believe computerized information files might be used to destroy individual freedoms; fifty-eight percent feel computers will be used in the future to keep people under surveillance; and forty-two percent believe there is no way to find out if

information about you stored in a computer is accurate. In general, the public believes government should make increased usage of computers in a number of areas, that such usage will make government more effective, and that there will, and should be, increasing governmental involvement in the way computers are used.

[29] Letter, identity withheld, in Subcommittee files with comment by the Director of the Federal Bureau of Investigation.

[30] 28 C.F.R. § 0.85 (b); codifying rulings by the Attorney General pursuant to 28 U.S.C. § 534 which provides:

(a) The Attorney General shall—

(1) acquire, collect, classify, and preserve identification, crime and other records; and exchange these records with, and for the official use of, authorized officials of the Federal Government, the States cities, and penal and other institutions.

(b) The exchange of records authorized by subsection (a) (2) of this section is subject to cancellation if dissemination is made outside the receiving departments or related agencies.

(c) The Attorney General may appoint officials to perform the functions authorized by this section.

[31] Morrow v. District of Columbia, 417 F. 2d 728 (D.C. Cir. 1969). For a summary of case law on this subject, *see* Longton, *Maintenance and Dissemination of Records of Arrest Versus the Right to Privacy,* 17 WAYNE L. REV. 995 (1971).

[32] Menard v. Mitchell, 430 F.2d 486 (D.C. Cir. 1970), *decision upon remand,* 328 F. Supp. 718 (D.D.C. 1971). The Court construed 28 U.S.C. § 534 narrowly to avoid the constitutional issues raised by *Menard* and found that:

It is abundantly clear that Congress never intended to, or in fact did, authorize dissemination of arrest records to any state or local agency for purposes of employment or licensing checks.

It found certain faults with the present system: (1) State and local agencies receive criminal record data for employment purposes whenever authorized by local enactment, and these vary state by state and locality by locality. (2) The Bureau cannot prevent improper dissemination and use of the material it supplies to hundreds of local agencies. These are no criminal or civil sanctions. Control of the data will be made more difficult and opportunities for improper use will increase with the development of centralized state information centers to be linked by computer to the Bureau. (3) The arrest record material is incomplete and hence often inaccurate, yet no procedure exists to enable individuals to obtain, correct or supplant the criminal record information used against them, nor indeed is there any assurance that the individual even knows his employment application is affected by an FBI fingerprint check.

The Court invited Congressional action, noting that: with the increasing availability of fingerprints, technological developments, and the enormous increase in population, the system is out of effective control. The Bureau needs legislative guidance and there must be a national policy developed in this area which will have built into it adequate sanctions and administrative safeguards.

[33] Congressional response to the District Court's invitation has taken several forms, among them, a bill, S. 2545, introduced, but not acted on, to authorize the Attorney General to exchange criminal record information with certain state and local agencies. Remarks by Senator Bible, S. 14558, 117 CONG. REC. (daily ed. Sept. 20, 1971); and an amendment to the Department of Justice Appropriation Act of 1972 temporarily restoring the power over arrest records limited by the *Menard* decision. 117 CONG. REC. S. 20461 (daily ed. Dec. 3, 1971). House Judiciary Subcommittee No. 4 on Mar 16 began hearings on H.R. 13315, a bill introduced by Rep. Edwards, "to provide for the dissemination and use of criminal arrest records in a manner that insures security and privacy."

A related, but more comprehensive bill, S. 2546, was introduced by Senator Hruska on Sept. 20, 1971, 117 CONG. REC. (daily ed.) to insure the security and privacy of criminal justice information systems. This is termed the Attorney General's response to an amendment to the Omnibus Crime Control Act of 1970, 18 U.S.C. §§ 351, 1752, 2516, 3731 (1964), requiring the Law Enforcement Assistance Administration to submit legislative recommendations to promote the integrity and accuracy of criminal justice data collection. LEAA demonstrated a prototype computerized system for exchange of criminal history information with the states, a project known as SEARCH—System for Electronic Analysis and Retrieval of Criminal Histories. In Dec. 1970, Project SEARCH was turned over to the FBI for the development of an operation system to be part of the National Crime Information System. The bill deals with criminal offender record information as well as criminal intelligence information.

A discussion of the philosophical, constitutional and legal issues and problems related to such a computerized system is found, with bibliographies, in *Security and Privacy Consideration* in *Criminal History Information Systems, Technical Rept. No. 2,* July, 1970, by Project SEARCH, California Crime Technological Research Foundation, funded by the Law Enforcement Assistance Administration, Department of Justice. Also pertinent is the testimony of LEAA officials on the use of information and intelligence systems by criminal justice agencies. *1971 Hearings,* on the National Crime Information Center. *Id.* at 914.

For a model state act proposed for criminal offender record information, *See generally Technical Memorandum No. 3,* May, 1971 by Project SEARCH.

As we have a highly mobile population, so we have a highly mobile criminal population, which requires that governments be able to share rapidly the information in their data banks in the interest of law enforcement. The problem is determining what agencies and what officials should control what information.

[34] *See 1971 Hearings* at 493–530. Testimony of Joseph Alioto, Mayor of San Francisco, and exhibits submitted. For response of Justice Department officials, see testimony of William Rehnquist, *id.* at 604, 878–88, and a series of memoranda from the Federal Bureau of Investigation, the Bureau of Narcotics and Dangerous Drugs, which memoranda were submitted by Assistant General Rehnquist with the caveat that.

Under the traditional notions of separation of powers, it seems to me probable that the Department could justifiably decline to furnish portions of this information . . . *Id.* at 1371.

[35] *1971 Hearings,* Part II at 1375. In his memorandum of Mar. 5, 1971, the Director of the Bureau of Narcotics and Dangerous Drugs noted" . . . it is possible that the documents or information in these four exhibits could have been passed to the LOOK reporters by a BNDD employee." He cites BNDD Order 0–98, May 27, 1970 as the Bureau's current public information policy and as essentially a restatement of 28 C.F.R. Pt. 50, § 50.2, which covers the dissemination of most types of information for the Department. However, he states that the strongest applicable regulations in this matter are found in 28 C.F.R. Pt. 45, § 45.735: "No employee shall use for financial gain for himself or for another person, or make any other improper use of, whether by direct action on his part or by counsel, recommendation, or suggestion to another person, information which comes to the employee by reason of his status as a Department of Justice employee and which has not become part of the body of public information."

Obviously, the disclosure of documents stamped "For official use only" would be contrary to this regulation if, in fact, the disclosures were made by Department of Justice employees.

[36] For statement submitted by a Special Agent of Military Intelligence and related correspondence, *see 1971 Hearings,* Part II at 1451–1457.

[37] *See generally Hearings on Psychological Tests and Constitutional Rights Before the Subcomm. on Constitutional Rights of the State Comm. on the Judiciary,* 89th Cong., 1st Sess. (1965) and *Hearings on S. 3779 on Privacy and the Rights of Government Employees,* 89th Cong., 2d Sess. (1969).

[38] *See 1966 Hearings, supra* note 37. In connection with a proposal introduced to protect the consttiutional rights of employees of the executive branch and to prevent unwarranted governmental invasion of their privacy, *see* Senate remarks of Senator Ervin ineluding discussion of need for law prohibiting requirements to reveal information on race, religion, national origin, personal family relationships, sexual attitudes and conduct and religious beliefs and practices in 112 CONG. REC. 16081, 18634 (1966), 113 CONG. REC. 4039, 10663, 27994 (1967), 114 CONG. REC. 11235, 17161, 19613 (1968), 115 CONG. REC. 2343, 117 CONG. REC. (daily ed. Apr. 1 and May 11, 1971). By such legislation, government may be prevented from intruding into protected First Amendment areas on subjects which should have nothing to do with the operation of a civil service merit system. By exclusion of such sensitive, subjective information from the computer systems, initially, government will be precluded from basing individual or general social judgments on outdated standards, changing mores, variants in ethnic, cultural or geographical backgrounds, or previous conditions of the individual's mind, heart, and personality. It will necessarily be confined to a consideration of current information relevant and pertinent to the problem at hand.

[39] *See generally Hearings on S. 1791 and Privacy, the Census and Federal Questionnaires Before the Subcomm. on Constitutional Rights of the Senate Judiciary Committee,* 91st Cong., 1st Sess. (1969) and hundreds of letters and complains about coercive statistical questionnaires. Appendix also contains judicial, legal and constitutional research materials as well as examples of many social and economic questionnaires. *See also* Pipe and Russell, *Privacy: Establishing Restrictions on Government Inquiry,* 18 AMER. UNIV. L. REV. 516 (1969). For a summary of the hearings, *see* Senate remarks of Senator Ervin, 115 CONG. REC. 17718 (1969). For possible political uses of such information acquired as economic and social indicators, *see* Report by House Government Operations Committee, Subcommittee on Government Information, on Department of Labor briefings on economic statistics; and 23 WESTERN POL. Q. 235 (1970). *See also* the finding and recommendations on privacy and confidentiality of the PRESIDENT'S COMMISSION ON FEDERAL STATISTICS (1971).

[40] *See 1969 Hearings, supra* note 39, testimony on behalf of the National Federation of Independent Business at 199, of attorney and farm owner William Van Tillburg at 74, W. Schliestett, businessman at 66, J. Cannon, attorney at 7,263.

[41] *Id.* at 830. Table of Census surveys of population and households, conducted for other government agencies, with indication of penalties and compliance techniques. In many of these, the data is kept on tape or film by both the Census Bureau and the

sponsoring agency, and the confidentiality rules of the sponsoring agency apply.

[42] *Id.*, at 251. Assistant Secretary of Commerce Chartener:

Assistant Secretary of Commerce CHARTENER. The wording deliberately has been rather subtle in its form. We never use the word "mandatory" on a questionnaire. Instead, people will be told that "your answer is required by law." In other cases, they may be told that a survey is authorized by law or it is important to your government or something of that sort. Now, the followup procedure is used not for purposes of coercion but rather in order to verify the correctness of an address.

Senator ERVIN. Do you not agree with me that such a procedure is designed to implant in the mind of the recipient of these questionnaires the impression that he is required by law to answer them?

Mr. CHARTENER. If it is a mandatory questionnaire that would be the case. In other instances, the repeated mailings which may go up to five or may involve telephone calls or even a personal call are simply a means of emphasizing the importance that the Government feels in getting this response . . .

The Department of Commerce opposed enactment of a simply-worded statute advising people that their responses to these statistical questionnaire were voluntary. *Id.* at 262.

Senator ERVIN. Would the Department of Commerce and its Bureau of the Census be opposed to enactment of Federal statutes which would require that the Bureau of the Census advise every citizen on a questionnaire sent out by the Bureau that where it is not required by law, not mandatory, this is an effort to elicit information desired by the Government on a voluntary basis?

Mr. CHARTENER. Senator, I think we would oppose that. This is a matter of rather subtle psychology. I do not think, personally, and this is the position of the Department, that we ought to go out of our way to tell people they do not need to bother filling out this questionnaire. . . .

Senator ERVIN. You think the statutes governing those questionnaires, which are mandatory and which are subject to the criminal penalty if not answered readily, are understandable by the average layman?

Mr. CHARTENER. I do not think any law is written to be readily understandable by the average layman. That is why we have lawyers.

But compare the testimony of the Secretary of the Department of Health, Education, and Welfare in the *1971 Hearings* at 788, opposing legislation, but favoring administrative notice of voluntariness for that Department's forms.

[43] 115 CONG. REC. 3356 (1969) and guidelines printed there. *See also* note 17, *supra*, correspondence and guidelines printed at 1541, *1971 Hearings*, Part II. *See* remarks of Rep. Stanton, 118 CONG. REC. at H208 (daily ed. Jan. 24, 1972) [Complaints Against Secret Service].

[44] Letter in Subcommittee files.

[45] *See Department of the Army Civil Disturbance Information Collection Plan*, May 2, 1969, collection priorities and requirements and distribution list for government agencies. Printed in *1971 Hearings* at 1126, 1136. This plan also appears with remarks of Senator Bayh, 117 CONG. REC. 2290 (daily ed., Mar. 2, 1971).

[46] Letters in Subcommittee files (identities withheld).

[47] Letter of inquiry from Subcommittee Chairman, July 6, 1971, citing the large number of reasons for which a person can receive an administrative discharge, ranging from family hardship to national security grounds, the inadequate procedures and safeguards surrounding such discharges, and the threat to individual freedom from unrestricted reporting of law-abiding citizens, who may become subjects of official surveillance through no fault of their own or of the Secret Service.

[48] This December 14, 1965 agreement between the Defense Department and the Secret Service was implemented within the Navy Department by SECNAV Instruction 5500.27, 18 March 1966, which contains a copy of the agreement. Administrative authority for this regulation is cited as Defense Dept. Directive 5030.34, dated 30 Dec. 1965; statutory authority for assistance to the Secret Service is cited as P.L. No. 90-331 (June 6, 1968) which provides for assistance to the Secret Service on request.

[49] Appendix B of Agreement. Under Appendix A, identification data, photograph, physical description, date and place of birth, employment, marital status and identifying numbers are to be furnished, together with summaries or excerpts from DOD files as applicable to an individual or group reported.

In a related exchange of correspondence, the Subcommittee Chairman, in response to complaints, directed an inquiry to the Secretary of the Navy, on April 22, 1970 about a Navy directive which required that in any case where enlisted personnel were to be separated under other than honorable conditions within the continental United States, local civil police authorities were to be notified in advance of the name, race, sex and place and date of birth of the person, and of the time and place such separation is to be effected. This regulation seemed to serve no useful function since the Army and the Air Force functioned without one. On May 7, 1970, the Navy Department notified the Subcommittee that they concurred in this view and would delete the reporting requirement. (Correspondence in Subcommittee files.)

[50] For legal and constitutional implications, as well as a comprehensive historical account, *see* testimony of Christopher Pyle, an attorney and former Captain in Army Intelligence. See 1971 Hearings at 147, and exhibits providing examples of nation-wide military surveillance.

[51] *See Ervin, Privacy and Governmental Investigations*, 1971 UNIV. ILL. L. FORUM 137 (1971) for an account of the various plans and their lack of relevance to the problem of putting down civil disturbances, and for analysis of the Defense and Justice Department's claims to constitutionality for the actions of the military. Texts of four "plans," *1971 Hearings* at 1123 1119, 1154, 1731; Memorandum at 1139. 1141, 1278-98, showing attempts by civilians to cut back on the program.

[52] The bulk of investigative activity by the Army's own personnel occurred at the field level. Agents collected information and filed "spot reports," "agents reports," and "summaries of investigation." Most of this data was forwarded up the chain of command but record copies were kept in data centers at every level of command. Manual files were maintained at every level. At least four and possibly more computer systems were employed to store, analyse and retrieve the information collected. Many files on lawful citizens were microfilmed and integrated with other files on persons who were suspected of violations of security and espionage laws. These computer systems were located in the headquarters of the Intelligence Command (Fort Holabird), the Continental Army (Fort Monroe), the Third Army Corps (Fort Hood), and in the Pentagon. More than one computer data bank was maintained in some of these locations. (Subcommittee investigation.)

[53] Testimony of Ralph Stein on the difficulty of labeling young people on the basis of their speech, when a difference of one digit was the difference between a communist and a non-communist. *1971 Hearings* at 248, 260.

[54] *See* Brief for Respondents filed in Tatum v. Laird in the Supreme Court of the United States, No. 71-288, challenging the Army's surveillance program, and arguing that plaintiffs' claims are justifiable and ripe for adjudication; that the present inhibiting effect on the exercise of First Amendment rights creates a justiciable controversy; that the justiciability of their claims is enhanced because the military exceeded its constitutional and statutory authority and intruded into civilian affairs; that they have standing to adjudicate these claims for themselves and the claims of others similarly situated; and finally, that they argue that their case cannot be mooted by the Army's assertion that its domestic surveillance activity has been reduced. The appendix contains an interesting and landmark study of the chilling effect of overbroad governmental programs on First Amendment activity from the social science view.

All of the plaintiffs named have been subjects of political surveillance, and all are believed to be subjects of reports, files, or dossiers maintained by the Army.

In an amici brief filed by Senator Ervin on behalf of the Unitarian Universalist Association, the Council for Christian Social Action, United Church of Christ, the American Friends Service Committee and the National Council of Churches of Christ, the question posed for review is framed as follows:

Do individuals and organizations not affiliated with the armed services present a justiciable issue under the First, Fourth, Fifth and Ninth Amendments when they allege that their rights of free expression, privacy and association have been infringed by unauthorized, unnecessary and indiscriminate military investigations of their political activities and personal lives? Brief for Respondents as amicus curiae at 7, Laird v. Tatum, No. 71-288 (1971).

Essential though the freedoms are, they are not easily exercised in a climate of fear, discord, and dissension, especially when the ideas being expressed are those which are displeasing to government and unsettling to the majority of citizens. . . . It is as such a time that the First Amendment is most necessary, most in danger, and most difficult to exercise. . . . The First Amendment however, was made for the timid as well as for the brave. While government cannot instill courage in the meek, it may not take advantage of a climate of fear to undertake a program which has the effect of restricting the First Amendment only to the very courageous, Government action, such as military surveillance, seemingly innocuous in the abstract, has the very real effect of suppressing the exercise of the First Amendment. The coercive power of this government action lies in the national climate of fear and doubt, and in the very real, tangible apprehension of some unknown form of retribution by government on those who it fears and therefore watches. That such apprehension exists in America today is manifest. *Id.* at 15.

[55] *1971 Hearings* at 765.

[56] *See* exchange of correspondence on this subject. *Id.* Part II at 1046 A, 1180 Indices to letters.

[57] *Id.* at 597, 849.

[58] *Id.* at 616-62.

[59] S. 1791, 91st Cong., 1st Sess. (1969).

[60] Senate remarks of Senator Ervin, 117 CONG. REC. (daily ed. June 24, 1971.)

[61] See S. Rep. 92-554 for legislative history (Now pending before the House Post Office and Civil Service Committee with House versions).

[62] *1971 Hearings* at 782 (complaints read into the hearing record by the Chairman).

[63] SOCIAL SECURITY NUMBER TASK FORCE REPORT to the Commissioner 17 (May, 1971).

[64] *Id.* at 15.

It is clear that if the SSN became the single number around which all or most of an individual's interactions with society were structured, and if practices of the sort we have been discussing were to continue, the individual's opportunity to control the circumstances under which information about

himself is collected and disclosed would be greatly circumscribed.

[65] *See* BOGUSLAW, THE NEW UTOPIANS (1965), especially the chapter entitled *The Power of Systems and Systems of Power* at 181, 186, 190. I would dispute his observation of some years ago that people in the information-processing profession "are scientists and engineers—objective experts whose only concern is technical efficiency and scientific detachment." *Id.* at 198. It is indeed true, however, that: to the extent that customers (and this may include government agencies or private industry) abdicate their power prerogatives because of ignorance of the details of system operation, *de facto* system decisions are made by equipment manufacturers or information-processing specialists. *Id.* at 198.

Implicit in the various issues raised during the Subcommittee Hearings is the wise observation of Professor Boguslaw that:

The paramount issues to be raised in connection with the design of our new computerized utopias are not technological—they are issues of values and the power through which these values become translated into action. *Id.* at 200.

In this case, I believe it is the constitutional value protected by the First Amendment.

[66] *See* note 53 *supra.*

[67] Towne v. Eisner, 245 U.S. 418, 425 (1918).

COMPUTERS AND PRIVACY: A PROPOSAL FOR SELF-REGULATION

(By Edward J. Grenier, Jr.*)

In framing the issues in its landmark Computer Inquiry, the Federal Communications Commission cited the critical importance of the preservation of information privacy:

"Privacy, particularly in the area of communications, is a well established policy and objective of the Communications Act. Thus, any threatened or potential invasion of privacy is cause for concern by the Commission and the industry. In the past, the invasion of information privacy was rendered difficult by the scattered and random nature of individual data. Now the fragmentary nature of information is becoming a relic of the past. Data centers and common memory drums housing competitive sales, inventory and credit information and untold amounts of personal information, are becoming common. This personal and proprietary information must remain free from unauthorized invasion or disclosure, whether at the computer, the terminal station, or the interconnecting communication link." [1]

Congress, too, has demonstrated an increasing concern with the possible threats to individual privacy which might result from the establishment, by the federal government or by private industry, of a national data bank.[2] In fact Paul Baran of Rand Corporation, testifying several years ago before a congressional subcommittee, stated that the United States is unconsciously moving toward an integrated, nationwide, automated information system:

"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." [3]

Although the threat posed by automated information systems to the privacy of *individuals* is perhaps the most dramatic aspect of the "computer revolution," another very important aspect is the possibility of unauthorized disclosure of *proprietary data*. The "privacy problem" in both of these contexts is most acute where the separate proprietary data of a large number of businesses or sensitive personal information about thousands of individuals is stored or processed in multi-programmed, time-sharing data processing systems and transmitted to and from the processing and storage units over common communications lines. In such systems, there exists at numerous points a high potential for "information leakage," including leakage due to hardware and software failures and wire taps.[4]

In addition to examining both of these aspects of the privacy problem from the point of view of the computer system operator, this article proposes the establishment of a logical legal framework which would serve the public interest by assuring, first, that computer systems which handle sensitive individual or proprietary data will meet certain minimum standards established for the protection of privacy, and, second, that computer system operators will be able to continue to operate in a competitive economy unhindered by either overly restrictive governmental regulation or the fear of private legal liability. The analysis and suggestions herein set forth are relevant to all types of computer systems which store information or use computer porgrams belonging to persons or entities other than the computer system operator or which collect and store information about private individuals.[5]

The computer industry, which when viewed in its broadest significance extends from manufacturers of main frame hardware to computer service bureaus and computerized information services, should now cooperate with the communications industry to adopt and implement, under the auspices of the federal government, a comprehensive system of self-regulation to ensure the privacy and security of data. As a corollary of such a scheme, computer systems complying with the established standards [6] should be freed from certain types of civil legal liability for the unauthorized or accidental divulgence of individual or proprietary information.[7]

THE PRESENT LEGAL SITUATION: A STUDY IN UNCERTAINTY

For the purpose of analyzing the present legal controls pertinent to privacy and the computer, it will be helpful to consider a few illustrative situations:

"1. Computer service company A operates a multi-programmed, time-sharing, remote-access data processing system. It services 25 customers scattered over a wide area, each with at least one remote terminal device. Each of A's customers stores at least one proprietary program and a good deal of data in A's system. Companies X and Y are competitors and are both customers of A. Let us suppose that company X has been able to obtain confidential data belonging to Y at X's remote terminal.

"2. Assume the same basic set of facts with the exception that A has 500 customers, most of which are very small.

"3. Company A runs a computerized information service containing personal data about thousands of individuals, including credit data, medical data, employment data, and educational data. A offers this service to carefully selected classes of subscribers, each of whom promises to use the information for only circumscribed and legitimate purposes.[8] Company A's subscribers are linked to its computer system by remote terminal. Mr. X, a nonsubscriber, manages to tap into company A's system and connect an unauthorized remote terminal, thereby gathering information about a number of individuals. The information so obtained is used in an article which he publishes in a national magazine.

"4. Assume the same facts as in example 3, except that a programmer-employee of company A, without authority, extracts information about some individual from the system and sells such information to Mr. X."

Although the number of possible variations is almost without limit, these four examples are sufficient to illustrate some of the difficulties which computer service companies may face.

From the point of view of the computer service company, the first two examples present issues of contractual or, possibly, tort liability.[9] The customer whose *proprietary* data has been obtained without authority by some third party might well have a claim for breach of contract against the computer service company. However, the results in such a situation can be quite diverse. If the computer service company is dealing with large, sophisticated customers, service contacts are likely to be thorough and well-defined, specifying with detail the degree of privacy and security of data promised by the company and expected by its customer. On the other hand, if the computer service company's customers are small and perhaps less sophisticated, the contract between them may tend to be of the boiler plate variety and may not contain provisions adequate to protect the privacy and security of data. But uncertainty, rather than a complete absence of protection, is more likely to be the case.[10] Unfortunately, the outcome in any specific situation will depend upon the prevailing business practices and governing standards in the state involved.

Examples 3 and 4 squarely raise the issue of the extent to which an *individual's* "right of privacy" will be afforded legal protection.[11] Although most privacy cases involving the disclosure of *individual* information are likely to arise as tort actions, situations could arise in which an individual might have a claim based upon the law of contract. For example, assume that a computer service company enters into a contract with company X to store personal data concerning some one thousand employees of X and to furnish the data to X upon request. Assume further that the contract includes specific provisions for protecting the privacy of the individuals involved. If the computer company breaches the contract by allowing information to fall into the hands of a third person who uses it to the injury of the employees, the injured employee might seek recovery against the computer service company as a third party beneficiary of the computer service contract.[12]

In most situations, however, an individual's claim that his privacy had been violated would have to be founded upon the tort of invasion of or interference with privacy. Although of relatively recent judicial recognition,[13] this tort has developed to the point where one noted commentator has been able to discern the existence of four separate torts under the rubric "invasion of privacy": [14] (1) unreasonable intrusion upon the seclusion of another or into his private affairs;[15] (2) appropriation of an individual's name or likeness;[16] (3) unreasonable publicity given to another's private life, or public disclosure of a private fact about an individual;[17] and (4) publicity which places another in a false light in the public eye.[18]

The tort doctrine regarding the protection of privacy, in its present state of development, quite possibly would not provide a basis for a finding of liability against the computer service company in either example 3 or 4, where we have assumed that the computer company took no deliberate action to injure the plaintiff. However, the law of privacy has developed in response to the changing conditions of society, and the advent of the computer age is almost certain to result in a further judicial expansion of the doctrine—perhaps with legislative help.[19] Although four states apparently still reject the right of privacy in its entirety,[20] judicial expansion of the doctrine continues. In *Griswold v. Connecticut*,[21] for example, the Supreme Court seemed to find, in a context quite far removed from the fourth amend-

---

Footnotes at end of article.

ment prohibition against unreasonable searches and seizures, a constitutionally protected right of privacy inherent in several amendments.[22]

Of special significance is the recent New York decision in *Nader v. General Motors Corp.*,[23] which extended the *Griswold* rationale prohibiting the violation of a constitutional right to privacy to invasions by a private corporations, not the state. The court implicitly found that state inaction—the refusal by the state court to entertain a lawsuit alleging a violation by the corporation of the plaintiff's constitutional right to privacy—constituted sufficient "state action" to invoke the protection of the fourteenth amendment.[24] If the holding in *Nader* survives, the implications for the computer industry could be far-reaching.[25]

There can be no doubt that the computer service industry, dealing as it does with personal data on hundreds or thousands of individuals, strongly affects the public interest.[26] Indeed, against the background of expanding computer services the need for a further extension of the doctrine of right of privacy has been vigorously asserted.[27] Thus, one commentator has recently noted that "[t]he concept of privacy held by most courts, considered revolutionary during the Warren-Brandeis era, seems more fitted for the 19th century rather than the 20th; a 'new privacy' must be formulated to protect the individual from the technological advances of the computer age." [28] Another commentator recently advanced the thesis that the fifth amendment prohibition against the taking of private property by the government without just compensation, applicable to the states through the fourteenth amendment, should be extended to a similar destruction or diminution of the right of individual privacy.[29] Furthermore, actions by large public corporations which result in a diminution of an individual's privacy should be regarded as equivalent to state action and therefore subject to the payment of "just compensation." [30] The growing tendency to extend the bounds of privacy protection is thus manifest.[31] If, because of their vast informational storage and ready access capabilities, computers and computer systems become generally regarded as great potential threats to the individual's right of privacy, it would not be surprising to find courts holding computer service companies liable for the unauthorized disclosure of information about an individual.[32] Moreover, the court might go beyond the traditional concept that the defendant must be guilty of an intentional or deliberate wrongdoing in order to be held liable under an invasion of privacy theory and hold computer companies liable for negligently permitting an unauthorized release of information. Indeed, if the information is sensitive enough and the damage from release is devastating enough, a court might be tempted to dispense even with the requirement of negligence and simply hold the computer company *absolutely* liable for the unauthorized release.[33] Whether the computer company's failure is technological [34] or human [35] should make no difference.

The law usually has evolved to keep pace with changing social, political, moral, and economic circumstances. For those who might dismiss as "mere speculations" the above thoughts about the possible evolution of the law of privacy in response to the computer revolution, it would be instructive to consider a statement by Professor Arthur Miller during a recent symposium on the computer and privacy:

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

"In short, I am suggesting that we are dealing with a problem of immense importance . . . . [G]iven the large stakes, we should not think simply in terms of the ethical or moral implications of a National Data Center, or any other type of a data center. We must recognize that we are dealing with a new technology, whose applications are just beginning to be perceived and whose capacity to deprive us of our privacy simply cannot be measured in terms of existing systems or assumptions about the immutability of the technology.[36]

It is apparent that the legal protection given to the right of privacy is far from static and may, within the reasonably foreseeable future, undergo marked changes. However, except insofar as the changes may be founded upon federal constitutional doctrines, the developing principles may vary markedly from state to state because the basic law involved will be state, not federal, law.[37] For the computer service company, this could mean facing different standards of liability in fifty different jurisdictions for the unauthorized disclosure of information—an unhappy prospect for companies who do a national or regional business.

At present, there is no body of federal law governing privacy which might "preempt" state law as applied to computer systems. After receiving the many detailed and thoughtful comments in its Computer Inquiry and the analysis of the responses prepared by the Stanford Research Institute, as well as the Institute's own recommendations, the FCC has decided that it must await the collection of additional information before deciding whether to exercise its regulatory authority in the area of privacy and security of data during transmission and storage.[38]

Although it did take a significant step in the privacy area in Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[39] Congress has not acted decisively in this area. In Title III, Congress (1) outlawed the interception and disclosure of wire or oral communications, except as specifically authorized in the statute pursuant to court order; [40] (2) amended section 605 of the Communications Act of 1934 [41] to take into account the foregoing addition to the federal criminal code; [42] and (3) established a "National Commission for the Review of Federal and State Laws Relating to Wire Tapping and Electronic Surveillance," which is to study the entire wiretapping and electronic surveillance situation and make a final report within seven years.[43] One interesting feature of this act is that it gives a civil cause of action for damages to "any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter. . . ." [44] Although this provision for civil damages in Title III will provide a new, and perhaps potent, remedy to the individual citizen in protecting his privacy, the remedy reaches only one aspect of the privacy problem in data processing, and it certainly does not in any way preempt the various provisions of state law dealing with invasions of privacy. First, the remedy is limited only to persons whose wire or oral *communications* [45] are intercepted, disclosed, or otherwise used in violation of the act. Thus, this remedy on its face does not reach the problem of the unauthorized disclosure of stored information about an individual, which is *not* "communicated" by the individual *himself* to someone else.[46] Secondly, it is not entirely clear whether the act's sanctions will even reach the problem of interception of data being transmitted to or from a data bank, or the disclosure of such data after interception. The term "intercept," as used in the act, means the "*aural* acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device." [47] Query whether transmitted data is subject to such "aural acquisition," at least in the case of data sent over a special digital communications network using time division multiplexing techniques; query whether courts would reach different conclusions depending upon the technical nature of the communications network over which the data traveled.[48]

A RATIONAL SOLUTION: SELF-REGULATION BY THE COMPUTER INDUSTRY UNDER GOVERNMENTAL AUSPICES

It is estimated that by the late 1970s, the traffic volume over the nation's telephone network will be about equally divided between voice and data transmission,[49] representing a far greater use of the telephone network for data transmission than at present. By 1975 more than 60 percent of the computer hardware used in the United States will be tied into the public communications system, and estimates for 1984 have run as high as 90 percent.[50] Thus, we are on the verge of an explosion in remote access data processing, including a great number of time-sharing, real-time systems. The trends in the law discussed above [51] may well be accelerated by the quickening pace of technological progress.

The choice lies with the computer industry. It can go along and let events unfold in an unstructured, haphazard manner and thereby permit others to fashion for it the basic standards and rules governing the conduct of its business, or it can itself initiate rational means to control its own destiny and at the same time serve the public interest by assuring privacy and security of data, in both transmission and storage. In an industry whose whole thrust is to bring rational order out of the potential chaos unleashed by the information explosion, the choice seems clear. Working from the foundations already laid, the computer industry should pull together, develop, and then enforce standards of construction and operation for computer systems which process data of such a nature that privacy or security are necessitated.

Before detailing the mechanics of this proposal it would be well to point out what is not being proposed. The regulation contemplated would not deal with such matters as the rates or prices to be charged by computer service companies, the rate of return they should earn, the terms and conditions of their sales to their customers, or other matters relating to traditional economic or rate regulation.[52] Rather, the industry, under federal governmental auspices, would develop standards to assure that computer systems will incorporate a reasonable degree of privacy protection and will be operated to achieve the desired degree of privacy and security of data necessary in any given circumstances.[53]

Any program of self-regulation should include at least the following features:

1. The program should be specifically authorized and established by federal statute, a prerequisite which would avoid the antitrust problems that inevitably arise where competitors or potential competitors associate to formulate industry standards.[54] Indeed, the statute should grant a specific antitrust exemption for activities within its scope.

2. Because the program is one of *self*-regulation, some statutory mechanism should be established to permit governmental administrative review of regulatory standards, upon the complaint of interested persons, before they become effective. Such a mechanism would provide customers and potential customers of the computer service industry, as well as private individuals, with

Footnotes at end of article.

an opportunity to express their views on proposed standards.[55]

3. An organization composed of representatives of the computer industry should be established to promulgate and enforce the desired standards. Such an agency should be specifically recognized and granted authoritative powers by federal statute, and its decisions in promulgating standards and in supervising the operations of the computer service industry should be final, though subject to specific types of review by an appropriate government administrative agency[56] and, ultimately, limited judicial review.[57]

4. The industry agency charged with promulgation and enforcement should have the power of periodic inspection to assure compliance with standards regarding the privacy and security of data.

5. The agency should have specific power at least to conciliate disputes between ustomers and computer service companies and between individual citizens and computer service companies, arising from, or related to, the standards formulated by the industry agency.[58] Perhaps such conciliation can be made a condition precedent to the bringing of any lawsuit involving the standards or application of the standards.[59]

6. The industry agency should, under guidelines set forth in the federal statute, establish a licensing or certification system for computer systems which will handle information about individual citizens or proprietary data belonging to persons or companies other than the computer system operator. Before any such computer system is permitted to commence operation, it should be required to obtain a license certifying that the industry standards for the protection of privacy and security of data have been met. Such standards should cover not only the technical aspects of the computer system, but also the qualifications of key personnel having access to the system. In connection with the licensing procedure, the applicant should be required to show that it has developed, and will use, appropriate procedures to comply with the standards and to assure that its key employees comply with the industry's code of conduct. As noted above, after initial licensing the industry's agency should have continuing inspection powers to assure that the licensee complies with industry standards. Again, both in connection with initial licensing and any subsequent industry proceeding brought to enforce compliance with standards, there should be review by the concerned governmental agency and, ultimately, limited judicial review. In the event of proposed major alterations in the system, a system licensee should be required to go through a new licensing procedure.

7. The industry agency should have power to promulgate and enforce a code of conduct for programmers and other key personnel working with computer system to which industry standards apply. Sanctions would be imposed upon individuals violating the code of conduct, subject, of course, to administrative review by a government agency and, ultimately, limited judicial review. Such sanctions might include the imposition of fines, with the maximum fixed by statute, suspension from employment, and, in the case of the most flagrant violations, even complete expulsion from the computer service industry.[60]

8. The federal authorizing statute should specifically provide that industry standards will be recognized and given full force and effect in all judicial proceedings, both state and federal. In fact, the statute should provide that, in the absence of an express agreement to the contrary between a computer service company and its customer, the company will not be liable for any loss or destruction of data, or "leakage" of data to unauthorized persons, if the company's computer system has been duly licensed and certified to be in compliance with the industry association's standards, and if in fact the system was in compliance with such standards at the time of the loss, destruction, or unauthorized disclosure. This same exemption from liability should apply, in the case of a claim against the computer service company by an individual on account of unauthorized disclosure of data about such individual.[61]

The preceding framework is necessarily a very broad-brush treatment of a highy complex subject. However, if the idea of self-regulation is accepted and adopted by the computer industry, the foregoing guidelines can be a point of departure in constructing the system. What is needed is a broad consensus within the industry as to the route to be followed, which can then be translated into concrete legislation and a detailed plan of operation.

On the technical side, considerable effort over the past few years has been devoted to developing and improving hardware and software techniques for assuring privacy and security of data during both transmission and storage.[62] In addition, many of the comments filed in the FCC's Computer Inquiry described various techniques used to assure privacy in remote access data processing applications.[63] Thus there is a readily available body of recorded experience and thoughtful comment upon which the standards makers could draw in beginning their complex task.

One aspect of the foregoing proposal for self-regulation must be given special attention. In the case of remote access data processing the communications links between the remote terminals and the computers must be considered a part of the computer "system" to be licensed or certified if there is to be really effective privacy protection. Yet, in virtually all instances, the communications links will be furnished by common carriers *not related* to the computer service company seeking the license or certification.[64] Thus neither the computer company nor the industry agency proposed above will have control over the degree of privacy protection afforded by a very important link in the computer "system" to be licensed or certified.

The solution to this problem does not rest in making the communications common carriers subject to regulation by the industry agency proposed in this article. Any regulatory scheme which subjects a company to regulation directly by its customers must be viewed with at least a healthy skepticism. Thus the communications common carriers should not be subject to regulation by the computer industry agency insofar as these carriers provide communications service in connection with remote access data processing.[65] Moreover, any such attempted regulation of the communications activities of the communications common carriers by the computer industry agency might well conflict with existing regulation by the FCC on the national level and by public service commissions on the state level.

Rather, the solution to the problem would appear to lie in a well-organized system of cooperation between the communications carriers and the computer industry agency, with regulatory assistance from the FCC as required. There should be a continuing formalized liaison between the communications carriers and the computer industry agency, perhaps in the form of one or more representatives of the communications industry working full time in the liaison activity. Such liaison could function effectively in at least two types of situations: (1) when the industry association is formulating privacy protection standards, it should consult closely with the communications industry to assure that tariffed offerings affording the desired degrees of privacy protection in various situations will be available to the computer service industry; (2) if communications problems arise in connection with any particular licensing proceeding under the above proposal, the suggested liaison could help to resolve the problem, possibly through inducing the carrier involved to make a new tariff offering or to amend an existing tariff offering.

Of course, if the liaison activity should fail to resolve any really significant problem, recourse could be had to the FCC or the appropriate state public service commission. To ensure that the FCC will be able to act effectively and expeditiously, the federal statute authorizing the system of industry self-regulation should expressly give the FCC whatever additional power that may be necessary.[66]

There is presently one highly successful example of industry self-regulation under federal governmental supervision. For some thirty years, the National Association of Security Dealers [NASD] has created and enforced a thorough program of self-regulation for the securities industry, including member broker-dealer firms and individual registered representatives. Its principal activities include the administration of examinations to assure the qualifications of employees in the securities industry, the promulgation and enforcement of rules of conduct and fair practice for the securities industry, and the adjustment of grievances between members and between members and the public.[67] One of the most effective tools in NASD's program of self-regulation is its power to examine the books and records of member firms to ensure compliance with NASD rules as well as certain federal regulations. This is equivalent to the inspection program proposed above for the computer industry. In addition, NASD operates a program of voluntary arbitration, both for disputes among its members and for disputes between the public and its members. In the case of disputes of the latter variety, the arbitration panel consists of three members of the public and two representatives from the securities business. In a member versus member contest, the panel consists of from three to five representatives from securities industry.

Although there are obvious differences between the securities industry and its problems and the computer industry and its problems, NASD constitutes a valid precedent for the type of self-regulatory industry agency proposed herein. By adopting a NASD-type approach, the computer industry can assure the creation of a rational and orderly legal framework for resolving the increasingly pressing problem of privacy in the context of the computer revolution and, at the same time, assure that regulation will be in the hands of persons thoroughly cognizant of the complexities of the situation and the need for protection of individual rights and proprietary interests in data and programs—all to the benefit of the public interest.

FOOTNOTES

* Member, District of Columbia Bar, B.A. 1954, Manhattan College; LL.B. 1959, Harvard Law School.

[1] FCC Notice of Inquiry, Docket, No. 16979, 7 F.C.C.2d 11, 16–17, 8 P & F RADIO REG. 2d 1567, 1572 (Nov. 9, 1966) [hereinafter cited as *Computer Inquiry*].

[2] *See generally Hearings on the Computer and Invasion of Privacy Before a Subcomm. of the House Comm. on Gov't Operations*, 89th Cong., 2d Sess. (1966) [hereinafter cited as *Gallagher Hearings*]; Note, *Privacy and Efficient Government: Proposals for a National Data Center*, 82 HARV. L. REV. 400 (1968); *Research Project—Computerization of Government Files, What Impact on the Individual?*, 15 U.C.L.A.L. REV. 1371 (1968).

[3] *Gallagher Hearings* 122.

[4] *See* Ware, *Security and Privacy in Computer Systems*, PROCEEDINGS, 1967 SPRING

JOINT COMPUTER CONFERENCE 279, 280 figure 1. Effective protection of both individual privacy and proprietary data also demands control over the amount and character of the data input entering the system. *See* Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society,* 67 MICH. L. REV. 1091, 1214–17, 1229–30 (1969) [hereinafter cited as Miller]. Regulation of data input is beyond the scope of this article which is directed solely to controls in the storage and utilization of the data previously collected.

[4] An obvious example of the latter is the automated credit bureau. Credit Data Corporation maintains a large scale, on-line computerized credit information system with data centers located in Los Angeles and New York City. Response of Credit Data Corp. to FCC Computer Inquiry, March 5, 1968. *See generally* Miller 1140–54.

[5] See notes 54–61 *infra* and accompanying text.

[6] This paper does not deal with the problems presented by the *voluntary* disclosure by the system operators of private information about individuals stored in computer systems or questions relating to the accuracy of information about individuals contained in such systems. For discussions of some of the problems involved in the storage of inaccurate information about individuals and the voluntary disclosure of information about individuals, whether accurate or inaccurate, by the custodians of such information, see Karst, *"The Files": Legal Controls Over the Accuracy and Accessibility of Stored Personnel Data,* 31 LAW & CONTEMP. PROB. 342 (1966); Sills, *Automated Data Processing and the Issue of Privacy,* 1 SETON HALL L. REV. 7 (1970); Note, *Credit Investigations and the Right to Privacy: Quest for a Remedy,* 57 GEO. L.J. 509 (1969).

[7] What constitutes "legitimate" voluntary disclosure of information by the information service company is beyond the scope of this paper. See not 7 *supra.*

[8] *See generally* Miller 1156–73.

[9] *See* Lickson, *Protection of the Privacy of Data Communications by Contract: Another Case Study on the Impact of Computer Technology on the Law,* BUS. LAW, July 1968, at 979–80.

[10] Under certain variations of these examples, the contractual rights of the computer service company's customer may also be involved.

[11] *See generally* RESTATEMENT OF CONTRACTS §§ 133–47 (1932).

[12] The Supreme Court of Georgia is considered to have laid the foundation for recognition of a right to privacy as a fundamental, legally protectible interest in Pavesich v. New England Life Ins. Co., 122 Ga. 190, 50 S.E. 68, 69–70 (1905). Of course, the intellectual foundation for recognition of invasion of privacy as a separate tort had been laid in Warren & Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 193 (1890).

[13] Prosser, *Privacy,* 48 CALIF. L. Law. 383, 389 (1960).

[14] *See e.g.,* Le Crone v. Ohio Bell Tel. Co., 120 Ohio App. 129, 201 N.E. 2d 533 (1963) (wiretapping of an individual's telephone).

[15] *See, e.g.,* Flake v. Greensboro News Co., 212 N.C. 780, 195 S.E. 55 (1938) (photograph of an actress used in a bread advertisement).

[16] *See, e.g.,* Brents v. Morgan, 221 Ky. 765, 299 S.W. 967 (1927) (sign in garage window stating that the plaintiff's account with the garage has been unpaid for a long time).

[17] *See, e.g.,* Peay v. Curtis Publishing Co., 78 F. Supp. 305 (D.D.C. 1948) (newspaper article on the alleged practices of Washington cab drivers in cheating the public on fares, making use of the plaintiff's photograph to illustrate the article).

[18] For example, Congress is now considering legislation which would regulate the activities of credit bureaus and credit investigating agencies, a field in which the computer has been playing an ever-increasing role. S. 823, 91st Cong., 1st Sess. (1969); H.R. 7874, 91st Cong., 1st Sess. (1969); H.R. 9150, 91st Cong., 1st Sess. (1969); H.R. 9888, 91st Cong., 1st Sess. (1969). The Senate passed S. 823 on Nov. 6, 1969, 115 CONG. REC. 13,905–11 (daily ed. Nov. 6, 1969) and reported it to the House Committee on Banking and Currency on Nov. 12, 1969. Hearings have been held this spring before the House Committee.

[19] These states are Nebraska, Rhode Island, Texas, and Wisconsin. RESTATEMENT (SECOND) OF TORTS, ch. 28A, at 100 (Tent. Draft No. 13, 1967).

[21] 381 U.S. 479 (1965).

[22] *See also* Tehan v. Shott, 382 U.S. 406 (1966), where the Court pointed out that the fifth amendment guarantee against self-incrimination is really in part an extension of an individual's right to privacy and "our respect for the inviolability of the human personality and of the right of each individual 'to a private enclave where he may lead a private life.'" *Id.* at 414 n. 12.

[23] 57 Misc. 2d 301, 292 N.Y.S. 2d 514 (Sup. Ct. 1968), *aff'd* 298 N.Y.S. 2d 137 (App. Div. 1969).

[24] *Id,* at 305, 292 N.Y.S. 2d at 518.

[25] The Appellate Division, in affirming the trial court's refusal to discuss the case, held that it need not pass upon the constitutional grounds advanced by the trial court, 298 N.Y.S. 2d at 141. We shall have to await further litigation to test the implications of *Nader.*

[26] *See generally* A. WESTIN, PRIVACY AND FREEDOM (1967); *Gallagher Hearings, supra* note 2; Pipe, *Privacy; Establishing Restrictions on Government Inquiry,* 18 AM. U.L. REV. 516 (1969); Note, *Credit Investigations and the Right to Privacy; Quest for a Remedy,* 57 GEO. L.J. 509 (1969); *Research Project—Computerization of Government Files, What Impact on the Individual?* 15 U.C.L.A.L. REV. 1371, 1375 (1968) (foreword by Mr. Justice Douglas).

[27] Note, *Credit Investigations and the Right to Privacy: Quest for a Remedy,* 57 GEO. L.J. 509 (1969).

[28] *Id.* at 532.

[29] Comment, *Privacy, Property, Public Use, and Just Compensation,* 41 S. CAL. L. REV. 902, 909 (1968).

[30] *Id.* at 913. The author's main point is made in the following statements:

"It can be argued that all large public corporations, such as Time, Inc., whose activity has as great a societal impact as does most governmental action, should be subject to the same constitutional limitations as is the government. Their activity should be labelled 'public,' rather than 'private,' in contradistinction to an individual's activity. . . . In short, most corporations are, at least in part, fulfilling interests of the state, and no longer fulfilling the traditional justifications of private property. In these instances they ought to be subject to the same constitutional limitations as are imposed that private property cannot be taken for a public use without payment of just compensation." *Id.* at 913–14.

And, as noted, the author would equate the "right of privacy" to "private property" and would require the payment of just compensation for any action which results in a destruction or diminution of an individual's right of privacy.

[31] The American Law Institute, in a tentative draft of a portion of a new Restatement of Torts, commented that new forms of the tort of invasion of privacy in addition to the four basic types already generally recognized by the courts may emerge, especially in light of recent decisions by the United States Supreme Court. RESTATEMENT (SECOND) OF TORTS § 652A, comment c (Tent. Draft No. 13, 1967). *See also* Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's, Pt. II: Balancing the Conflicting Demands of Privacy, Disclosure, and Surveillance,* 66 COLUM. L. REV. 1205, 1232 (1966).

[32] This might prove true whether the companies are service bureaus, information services, or some other type of computer service company.

[33] Early manifestations of the theory of strict liability are shown in Huthringer v. Moore, 31 Cal. 2d 489, 190 P.2d 1 (1948); Ball v. Nye, 99 Mass. 582 (1863) (percolation of filthy water); Cahill v. Eastman, 18 Minn. 324 (1872) (underground water tunnel). For an example of statutory extension of this principle, see the relevant portions of the Federal Safety Appliance Act, 45 U.S.C. §§ 1–60 (1964).

[34] See, for example, situations 1, 2, and 3, text at 497.

[35] See, for example, situation 4, text at 497–98.

[36] *Symposium: Computers, Data Banks, and Individual Privacy,* 53 MINN. L. REV. 211, 225–27 (1967). The growing concern over protecting privacy in our era of technological explosion is evidenced by the fact that most of the May-June 1969 issue of THINK, the very informative magazine published by IBM, is devoted to a special report on privacy. The articles include Miller, *Psychological Testing: Can We Minimize the Perils?,* THINK, May-June 1969, at 24; Ruggles, *How a Data Bank Might Operate, id.* at 22; Westin, *Life, Liberty, and the Pursuit of Privacy, id.* at 12; Westin, *New Lines Will Protect Your Privacy, id.* at 27. Professor Westin's concluding remarks in his first article are especially illuminating: "American Society now seems ready to face the impact of science on privacy. Failure to do so would be to leave the foundations of our free society in peril." Westin, *Life, Liberty, and the Pursuit of Privacy, id.* at 21. In his second article, Professor Westin points out that many organizers of private data banks, in growing recognition of the privacy problem presented by the computer revolution, are establishing administrative controls to assure the protection of privacy. Westin, *New Laws Will Protect Your Privacy, id.* at 31.

[37] *See* Erie R.R. v. Tompkins, 304 U.S. 64 (1938), which laid to rest the notion that there is any generally applicable federal common law to be applied by the federal courts in considering "general" issues in diversity cases. For a more thorough discussion of the *Erie* line of cases, see 1 A. J. MOORE, FEDERAL PRACTICE ¶ 0.318 (2d ed. 1965); Friendly, *In Praise of Erie—And of the New Federal Common Law,* 39 N.Y.U.L. REV. 383 (1964).

[38] *Computer Inquiry,* Report and Further Notice of Inquiry, 17 F.C.C. 2d 587, 592, 16 P & F RADIO REG. 2d 1505, 1510 (1969); *Computer Inquiry,* Notice of Proposed Rule Making and Tentative Decision, 18 P & F RADIO REG. 2d 1713, 1718 (1970). The regulatory authority of the FCC in this area may, of course, be limited in the absence of additional legislation.

[39] 18 U.S.C. §§ 2510–20 (Supp. IV, 1969).

[40] *Id.* §§ 2511, 2515–19.

[41] 47 U.S.C. § 605 (Supp. IV, 1969).

[42] § 803, 82 Stat. 212, 223 (1968) (reprinted in full following 18 U.S.C. § 2510 (Supp. IV, 1969)).

[43] § 804, Stat. 212 223–25 (1968) (reprinted in full following 18 U.S.C. § 2510 (Supp. IV, 1969)).

[44] 18 U.S.C. § 2520 (Supp. IV, 1969).

[45] As used in the statute, "wire communication" means:

any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications. *Id.* § 2510(1).

An "oral communication" means: "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." *Id.* § 2510(2).

[46] *See* Miller 1201.

[47] 18 U.S.C. § 2510(4) (Supp. IV, 1969) (emphasis added). It remains to be seen how the definition will be interpreted. The legislative history of the Act shows clearly that Congress was preoccupied with the interception of voice communications, whether by wiretapping or other electronic devices. *See* S. REP. No. 1097, 90th Cong., 2d Sess. 217–218 (1968). The few cases that have cited Title III of the Act have all been criminal cases or civil antitrust cases closely related to criminal cases and have all dealt with voice communications. *See, e.g.,* Alderman v. United States, 394 U.S. 165, 175 & nn. 8–9 (1969); United States v. McCarthy, 292 F. Supp. 937, 943 (S.D.N.Y. 1968); Philadelphia Housing Authority v. American Radiator & Standard Sanitary Corp., 291 F. Supp. 247, 249–50 (E.D. Pa. 1968); United States v. Schipani, 289 F. Supp. 43, 60 (E.D.N.Y. 1968); United States v. American Radiator & Standard Sanitary Corp., 288 F. Supp. 701, 706–07 (W.D. Pa. 1968).

[48] For example, the courts might arguably distinguished between interception of data transmitted by the regular analog telephone network and that carried over a special digital network. *See generally* Miller 1206.

[49] *See* Chaney, *Data Transmission Basics,* COMMUNICATIONS, Mar. 1969, at 27; *cf.* Irwin, *Computers and Communications: The Economics of Interdependence,* 34 LAW & CONTEMP. PROB. 360, 361 (1969).

[50] Note, *Computer Services and the Federal Regulation of Communications,* 116 U. PA. L. REV. 328 (1967).

[51] See notes 13–17 *supra* and accompanying text.

[52] The respondents to the FCC's Computer Inquiry, including the Department of Justice, generally agreed that the computer service industry should be permitted to develop in the free competitive economy, and not as a regulated utility. *See* L. KRAUSE, *Analysis of Policy Issues in the Responses to the FCC Computer Inquiry,* STANFORD RESEARCH INSTITUTE, REPORT No. 7379B–2, at 22–26 (1969). The author agrees. For a thorough discussion of the issues involved, see S. MATHISON & P. WALKER, COMPUTERS AND TELECOMMUNICATIONS: ISSUES IN PUBLIC POLICY 16–19 (1970). The FCC as of this time, agrees. *See Computer Inquiry,* Tentative Decision, 1718–22.

[53] These standards should be defined to the greatest extent possible.

[54] For a discussion of the limitation imposed by the federal antitrust laws on schemes of self-regulation within an industry, see Silver v. New York Stock Exchange, 373 U.S. 341 (1963), where the Court cautioned that such schemes will be closely scrutinized because of their potential effect on competition within the industry. *See generally* G. LAMB & S. KITTELLE, TRADE ASSOCIATION LAW AND PRACTICE §§ 11.1-.9 (1956); Baum, *Self-Regulation and Antitrust: Suppression of Deceptive Advertising by the Publishing Media,* 12 SYRACUSE L. REV. 289 (1961); Rockefeller, *Industry, Efforts at Self-regulation,* 10 ANTITRUST BULL. 555 (1965); *Developments in the Law—Deceptive Advertising,* 80 HARV. L. REV. 1005, 1159–63 (1967).

[55] Such a procedure would afford roughly the same right to comment as is now granted by section 4 of the Administrative Procedure Act, 5 U.S.C. § 553 (Supp. IV, 1969), which provides for the filing of written comments, after appropriate notice, in the case of administrative agency rule making.

[56] The author has deliberately refrained at this time from suggesting what government agency should undertake this function. The FCC, with its broad expertise in the communications field, might be the most logical candidate. Perhaps a new agency under the Department of Commerce might best do the job. In any event, the Congress, in selecting or creating the agency to do the job, should take meticulous care to assure that the agency and the whole regulatory scheme will work in tandem with a well defined national communications policy, as well as in furtherance of national policy in the privacy area. *See generally* Miller 1236–39.

[57] *Cf.* Silver v. New York Stock Exchange, 373 U.S. 341 (1963), where the Court utilized the federal antitrust laws as a basis for its review of the procedural integrity of a system of industrial self-regulation.

[58] It may be appropriate to provide for binding arbitration of such disputes instead of merely conciliation. This would be feasible, however, only if the industry agency were a truly independent authority and had such status and reputation for objectivity that nonmembers of the computer service industry would regard it as a fair tribunal.

[59] *See generally* W. GELLHORN & C. BYSE, ADMINISTRATIVE LAW 649–51 (4th ed. 1960). For a discussion of the utility of the conciliation process in an analogous context, see 1968 DUKE L.J. 1000 (conciliation procedure in an Equal Employment Opportunity Commission proceeding).

[60] Theft of a computer program might be ground for such expulsion. In at least one case, a court has held that computer programs are "property" subject to "theft" under state law, and an employee of a computer company who stole such programs was guilty of felony theft. Hancock v. State, 402 W.2d 906 (Tex. Crim. App. 1966).

[61] To reiterate, there should be no statutory exemption from liability in the case of voluntary and deliberate acts by the computer service company including companies offering computerized information services. At least as this author now envisions the proposed industry association, it would not deal with criteria for the voluntary release of information to "interested persons," government agencies, or other individuals, groups, or organizations. It may well be that, as the system develops and considerable experience is gained with the arrangement proposed in this article, it will eventually be appropriate for the industry association to promulgate standards governing the voluntary disclosure of information. Of course, to be really effective, especially against the federal government itself, the association should have specific federal statutory authority to promulgate and enforce such standards, and the statute should expressly make them applicable to government agencies.

[62] For example, three excellent papers summarizing some of the problems involved in achieving privacy and security of data in multi-programmed computer systems were presented at the 1967 Spring Joint Computer Conference. PROCEEDINGS, SPRING JOINT COMPUTER CONFERENCE 279–90 (1967). The individual articles were Peters, *Security Considerations in a Multi-Programmed Computer System,* id. at 283; Ware, *Security and Privacy in Computer Systems, id.* at 279; Ware, *Security and Privacy: Similarities and Differences, id.* at 287. The terms "security" and "privacy" are used in special senses in those papers, as summarized by Willis Ware in the last-cited paper: "For the purposes of this paper we will use the term 'security' when speaking about computer systems which handle classified defense information which nonetheless must be protected because it is in some respect sensitive." *Id.* The term "security" has been used in a broader sense throughout this article.

[63] *See, e.g.,* Response of United States Department of Justice (Mar. 5, 1968), filed in Computer Inquiry, FCC Docket No. 16,979.

[64] *See* Irwin, *supra* note 49, at 360–61 (1969); Miller 1099–1103.

[65] However, if the carriers utilize separate subsidiaries to engage in computer service operations which would be subject to regulation by the industry association if performed by computer companies not related to communications common carriers, such carriers or their computer service subsidiaries should be subject to industry regulation in the privacy area.

[66] Even if the FCC might be able to act pursuant to its existing general powers under the Communications Act of 1934, 47 U.S.C. §§ 151–609 (1964), there may be considerable advantage in spelling out the FCC's jurisdiction in this situation and perhaps providing for special streamlined procedures.

If the FCC is to become involved in a significant way in this situation, perhaps it should be the agency to review actions of the computer industry agency although Congress might wish to consider other alternatives before determining whether to give such jurisdiction to the FCC. See note 56 *supra* and accompanying text.

[67] This description of the NASD and its activities is taken from the 1968 NASD President's Report. 1968 NASD ANN. PRESIDENT'S REP. Of interest to the computer industry in formulating its system of self-regulation might be the NASD's statement of purposes:

(1) To promote . . . the investment . . . and securities business, to standardize its principles and practices, to promote . . . high standards of commercial honor, and to . . . promote among members observance of Federal and State securities laws;

(2) To provide a medium through which its membership may . . . consult, and cooperate with governmental and other agencies in the solution of problems affecting investors, the public, and [this business] . . .;

(3) To adopt . . . and enforce rules of fair practice [in the securities business] . . . and in general to promote just and equitable principles of trade for the protection of investors;

(4) To promote self-discipline among members, and to investigate and adjust grievances between the public and members . . . CCH NASD MANUAL ¶ 1003.

With some slight change in terminology, many of these statements might be substantially adopted by the computer industry.

ANNOUNCEMENT OF HEARINGS ON S. 6, EDUCATION FOR ALL HANDICAPPED CHILDREN

Mr. RANDOLPH. Mr. President, as chairman of the Senate Subcommittee on the Handicapped, I announce that our subcommittee will conduct hearings on S. 6, a bill for the education of all handicapped children. The hearing will be held on Monday, June 17, 1974, at 9 a.m. in room 4232, Dirksen Senate Office Building. Persons wishing to present statements should contact Mrs. Patria Forsythe, professional staff member, or Miss Anne Hocutt, research assistant, Subcommittee on the Handicapped, at 202—225–9075.

NOTICE OF HEARING ON RURAL ENVIRONMENTAL ASSISTANCE PROGRAM AND RURAL ENVIRONMENTAL CONSERVATION PROGRAM

Mr. HUDDLESTON. Mr. President, the Subcommittee on Agricultural Production, Marketing, and Stabilization of Prices of the Committee on Agriculture and Forestry will hold a hearing Thursday, June 20, on implementation of the rural environmental assistance program—REAP, and the rural environmen-

tal conservation program—RECP, beginning at 10 a.m. in room 324, Russell Office Building. The subcommittee will review the operations of the Soil Conservation Service to determine the reasons for reports of inadequate technical assistance being given our farmers. Anyone wishing to testify should contact the committee clerk as soon as possible.

NOTICE OF HEARING ON NOMINATIONS

Mr. ROBERT C. BYRD. Mr. President, on behalf of the Committee on the Judiciary, I desire to give notice that a public hearing has been scheduled for Wednesday, June 19, 1974, at 9:30 a.m., in room 2228, Dirksen Senate Office Building, on the following nominations:

William H. Orrick, Jr., of California, to be U.S. district judge, northern district of California, vice William T. Sweigert, retired

Henry F. Werker, of New York, to be U.S. district judge, southern district of New York, vice Sylvester J. Ryan, retired

At the indicated time and place persons interested in the hearing may make such representations as may be pertinent.

The subcommittee consists of the Senator from Mississippi (Mr. EASTLAND) chairman; the Senator from Arkansas (Mr. MCCLELLAN), and the Senator from Nebraska (Mr. HRUSKA).

NOTICE OF HEARING ON PRESIDENT'S NOMINATION OF DR. JOHN C. SAWHILL TO BE ADMINISTRATOR OF FEA

Mr. JACKSON. Mr. President, a second day of hearings on the President's nomination of Dr. John C. Sawhill to be the Administrator of the Federal Energy Administration has been scheduled for Wednesday, June 12, at 2 p.m.

The purpose of this second day of hearings on this important position is to permit Members who were unable to be present at the hearings on Friday, June 7, to appear and propound questions to Mr. Sawhill.

Further information concerning the location of the hearings will be available tomorrow morning at the office of the Senate Committee on Interior and Insular Affairs.

NOTICE OF HEARINGS ON RADIATION HEALTH AND SAFETY ACT OF 1973

Mr. KENNEDY. Mr. President, I want ot take this opportunity to announce Senate Health Subcommittee hearings on S. 667, the Radiation Health and Safety Act of 1973, which will be chaired by my good friend and colleague, Senator JENNINGS RANDOLPH. These hearings will be conducted on June 19, 1974, and will begin at 10 a.m. Persons interested in testifying should contact Mr. Richard Grundy at 225-9894.

ADDITIONAL STATEMENTS

SENATOR CURTIS CALLS FOR FAIRNESS IN THE CONSIDERATION OF CHARGES AGAINST PRESIDENT

Mr. HELMS. Mr. President, this past Sunday the distinguished Senator from Nebraska (Mr. CURTIS) addressed a meeting in Washington of the National Citizens' Committee for Fairness to the Presidency.

In his customary forthright fashion, Senator CURTIS gave his analysis of the existing situation concerning charges leveled at the President of the United States by the major news media, various committees of the Congress, and others.

Senator CURTIS calls for fairness, Mr. President, and I think all Senators, regardless of political affiliation, will be interested in the eloquent remarks by our distinguished colleague.

Therefore, Mr. President, I ask unanimous consent that the text of Senator CURTIS' address be printed in the RECORD.

There being no objection, the address was ordered to be printed in the RECORD, as follows:

SPEECH OF SENATOR CARL T. CURTIS

Mr. Chairman, distinguished guests: My heart swells with gratitude for the dedicated work of the Committee created to defend the Presidency of the United States. I am grateful for their work and the like work of all others. I believe that they are fighting the cause not only of our country but of free men everywhere. To you, Rabbi Korff, I say thank you very much. Americans will always be grateful for what you are doing.

We have a tough fight on our hands but in my opinion, the "get Nixon crowd" including those who continue to conduct a trial by press are in for a big surprise. They are losing their case. As I travel up and down this country, I am convinced that the vast majority of the people who do the work of the country, who pay its taxes and who fight its wars, are with the President of the United States, Richard M. Nixon.

We are, however, in an all-out fight. We are opposing a loud and determined group. They are a powerful group and they have at their command tremendous propaganda weapons. We must take our message to the people.

The American people need to be reminded that they have a President who wants to get on with the business of strengthening the country. He wants to restore financial sanity to the Federal Government. He wants to curb inflation. And these things, I submit, are vital to the very survival of our nation. We will fail to do them at our peril.

The people of the entire free world look upon President Nixon as their leader. They do so with good cause. President Nixon is the world's foremost and most successful peacemaker.

I cannot forget that when Mr. Nixon was sworn in as President our casualties in Vietnam were running as high as 300 a week. They were gradually reduced and finally brought to zero. Our combat troops have been removed from Vietnam, prisoners of war have been brought home, and young men are no longer drafted into the Army.

Neither can I forget the cruel criticism, the unfounded charges, the shameful accusations that were heaped on President Nixon throughout the months that he was doing so much for our country to end the war which he didn't start. There were marches upon Washington and his critics missed no opportunity to hinder and thwart his actions.

Let us consider the Middle East. This is an area of the world which has been torn by war and strife for a long time now. The feelings and bitterness run very deep, yet it is all changing now. The fighting has stopped. There has been a withdrawal of troops. The killing has ended. There has been an exchange of prisoners of war and the parties are proceeding to negotiate a peace.

Oh, yes, we will forever be grateful for the skill, the dedication and the tenacity of our Secretary of State, Dr. Henry Kissinger. A Secretary of State can only accomplish those things which are in the plan of the President who appoints him and directs him. The power and the might of a country are essential weapons in all diplomatic dealings. In the United States there is only one person who speaks in matters of foreign affairs and who is Commander in Chief of our armed forces. That man is the President of the United States. Because we have a strong and wise President, and a President who has dedicated his life toward a generation of peace, it has been possible for this country of ours to benefit from the skill and talents of a great Secretary of State.

Most of us know of the joy that has come to the mothers, wives, fathers and children of the American servicemen when wars have ended for us. No doubt greater joy has come to the peoples on all sides in the Middle East now that they are experiencing peace and a justified hope that it will become permanent.

I have served in Congress throughout World War II, the Korean War, and the Vietnam War, and I am not going to turn my back on Richard Nixon, the peacemaker.

Few people can appreciate the burdens on the President of the United States. Every Congressman and every Senator must delegate matters to his staff that he would like to do himself. Our responsibilities and the size of our constituencies are such a small fraction of those of the President. There are always tremendous burdens falling on the President in reference to domestic matters.

1972 was a momentous year in President Nixon's accomplishments in world affairs. The Vietnam War was being wound down, leading to its total halt. This called for courageous and soul-searching decisions as to bombing and other actions. The President's visits to Mainland China and to the Soviet Union were handled by him with great expertise.

His 1972 campaign had to be managed by others. I am convinced that President Nixon not only was not involved but never condoned any wrongdoing and that the real facts were withheld from him far too long.

Most citizens are aware that the President of the United States has been ruthlessly subjected to a trial by press, that the American principle of presumption of innocence and that testimony should be taken under oath and subject to rigid cross-examination, have not been followed. What about the principle that an accused person must be found guilty beyond a reasonable doubt?

Congressional committees have been used to advance the publicity of aspiring politicians. These committees have provided forums for the spreading of hearsay and unsubstantiated charges.

A grand jury in Washington has been at work, the makeup of which can hardly be described as a cross-section of our country. The very atmosphere in Washington is not conducive to a fair trial.

A special prosecutor has worked with a staff selected by his predecessor. I think I am quite charitable when I say that Archibald Cox is not noted for being non-partisan nor for being objective.

During the 1960 Presidential campaign, Mr. Cox was described as the "informal dean of the Kennedy Brain Trust." In 1973 he proceeded to assemble a prosecutor's staff without any political balance whatever. His Deputy was Henry S. Ruth, who served under Robert Kennedy when he was Attorney General. One of his assistants, James Vorenberg, served on the McGovern staff when McGovern was running for President. He was a frequent critic of President Nixon's law and order pronouncements and had served under Attorney General Robert Kennedy.

Philip B. Heymann, who was on Cox's staff, was an assistant to the solicitor general during the Kennedy and Johnson Adminis-