DATA BANKS PRIVACY AND REPRESSION

DONATION: 50¢

egislator Seeks Curb

Army Tracks Down

On Federal Data Bank

'Missina' Data Ban

EXPERTS QUESTION USE OF DATA BANK

Computerized Law

Police Files

Grows

come Bill

Dossier Fil

Data Bank

Dissenters

net Chiefs

lain Snoops

me Spying

Federal Computers Amass Dossiers on

of Thousands of Citizens

Computer People for Peace The Dolphin Center
137a West 14 Street New York City 10011

THE FUTURE EMPLOYMENT INTERVIEW

Mr. George Miron, an experienced systems analyst, is applying for a job at a consulting firm. A senario of the interview follows.

INTERVIEWER: "Good morning. My name is Herman Klutz. Have a seat, Mr. Miron."

APPLICANT: "Thank you."

INTERVIEWER: "Can I have your social security number, please."

APPLICANT: "It is nine two four, dash, six two, dash, four nine nine nine."

INTERVIEWER: "Thank you."

The interviewer has a computer terminal at his desk and keys in the applicant's social security number and the classification code for the Systems Analyst position the applicant is being considered for. After about 30 seconds the terminal starts humming and prints out the following message:

APPLICANT - GEORGE MIRON SOCIAL SECURITY # 924-62-4999
JOB HISTORY - FULLY ACCEPTABLE
PERSONAL HISTORY - NOT ACCEPTABLE

INTERVIEWER: "I'm sorry, Mr. Miron, but our computer analysis of your dossier from the National Data Bank Files says that you are not acceptable for employment at our company."

APPLICANT: "What could be on my file that makes me not acceptable?"

INTERVIEWER: "I'm sorry, Mr. Miron, the computer says that your job history is acceptable but your personal history is not. If you feel that there is something on your file in error you can try to have that corrected. We will reconsider you at that time if another position opens up."

APPLICANT: "Mr. Klutz, I am positive that my personal history is untarnished. It must be recorded incorrectly. Trying to get something corrected on the National Data Bank File takes at least several months and involves a lot of time and money. I've just been laid off and I need another job now."

INTERVIEWER: "I'm sorry, Mr. Miron, but it is company policy and the policy of most businesses to rely on the information in the National Data Bank in our hiring decisions. We can't afford to take any chances."

"THE BIG BROTHER OF 1984 MAY NOT BE A GREEDY POWER-SEEKER, BUT RATHER A RELENTLESS BUREAUCRAT OR OPPORTUNIST OBSESSED WITH EFFICIENCY, WHO MAY USE INFORMATION FOR PURPOSES OTHER THAN THOSE FOR WHICH IT WAS COLLECTED"
Jerry Rosenberg, The Death of Privacy, page 20

INTRODUCTION

An individual's control over information regarding his or her mental health record, political affiliations, educational information, selective service records, financial history, employment records, personal tastes and attitudes, friends and associations, and other aspects of one's life should not be taken away. For someone else to have this control would allow the other person or agency to make decisions about people's lives and deny them their basic rights.

The First Amendment to the Constitution prohibits Congress from:

> "...abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble and to petition the Government for a redress of grievances."

When one cannot exercise any of these freedoms without being subject to the surveillance and record-keeping of governmental or private agencies, one loses these freedoms to a repressive force.

The Fourth Amendment states:

> "The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, shall not be violated."

How can people be secure in their persons when they do not know what information is being compiled about them, by whom and for what purposes? This kind of action contributes to rising insecurity and paranoia in our people.

The Fifth Amendment states:

> "No person shall ... be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."

When personal data is used by others without the consent or knowledge of the person involved, one is being deprived of one's constitutional rights.

Repression is the state of keeping under control, checking or suppressing; the reducing of people to subjection. A data bank is a collection of records, one of which might very likely be yours. Some of the data banks your dossier might appear in are: school, employment, unemployment, bank, insurance company, health, credit, social security, welfare, census, IRS, secret service, police, FBI, Army, plus many others (Think of how many you can come up with!).

This information at the fingertips of others reduces one to a state of subjection (it restricts one's right to make personal decisions freely), works to keep people under control, checked and quiescent (it restricts one's right to freely petition the government, freely express grievances, freely control one's destiny). In other words, data banks breed repression.

Unfortunately, the scope of this booklet does not allow us to go into a detailed analysis of the abuses and possible cures of the concept of data banking. It is intended to provide an overview of the types of information now being collected about us; the ramifications of computer technology on the distribution and collection of this information; and the legal pitfalls we will confront in curtailing both the collection and distribution. For more detailed analysis, a list of suggested readings is appended.

"Removing the right to privacy can lead to a conforming society fearful of experimenting with the challenges of the day."
Rosenberg, The Death of Privacy, xii

	Surveillance Systems	Record Keeping Systems
Government Collection Agencies	Army Justice Department Secret Service	Internal Revenue Post Office Health, Education, Welfare Census Bureau
Commercial Collection Agencies	Credit Agencies Private Dectectives	Medical Records Employment Insurance Banks

"The end result of a "dossier society" is no less inimical to individual liberty if it comes from uncontrolled and unrestrained computerization of our citizens for benevolent ends such as traffic safety, welfare, improved criminal justice, and other socially beneficial programs."
Senator Sam J. Ervin (D., N.C.)

COMPUTER MYTHOLOGY

Although the cry "the computer is just a tool" can be heard from one corporation to the next, those of us in the industry know that the use of this tool has far outstripped our ability to control it. This is not to say that the machine is now thinking for people, for we are not there yet. But we have approached the point where we have allowed advances in technology to lead us to the development of systems which are so large that even the designers can not handle the whole problem.

To the lay person, computers are impersonal beasts, who always make mistakes and are therefore the enemy. This image clearly did not arise out of thin air. Computers <u>are</u> impersonal and as we now know they not only make mistakes when programmed to do so, but invade our lives with a constant accumulation of electronic tracks.

There can be little question that computers, do in fact magnify the problems of data banking. Although there are many private and government dossier files which are manually kept, the advantages of computers--their speed and storage capacity--are tempting to anyone interested in collecting information. In late April of this year tape storage equipment was announced which has the capacity to store a dossier on every living person in the United States and retrieve any one record in a maximum time of 28 seconds. Even without this new capacity, the Department of Defense has managed to limp along and compile a file of 25 million names, using equipment which is almost ten years old (the IBM 1401). This file, sometimes known as the

Index of Personnel Security Files, lists information about each person who has applied for security clearance, including private as well as governmental employees.

People who do not work with computers every day are often confused over the role that the equipment itself plays and the tasks that must be performed by programmers and other computer personnel. This confusion is intensified by the image that the computer industry tries to portray. The industry spends millions each year on public relations, depicting the "touch of a button" capabilities of their equipment. It's not quite that easy.

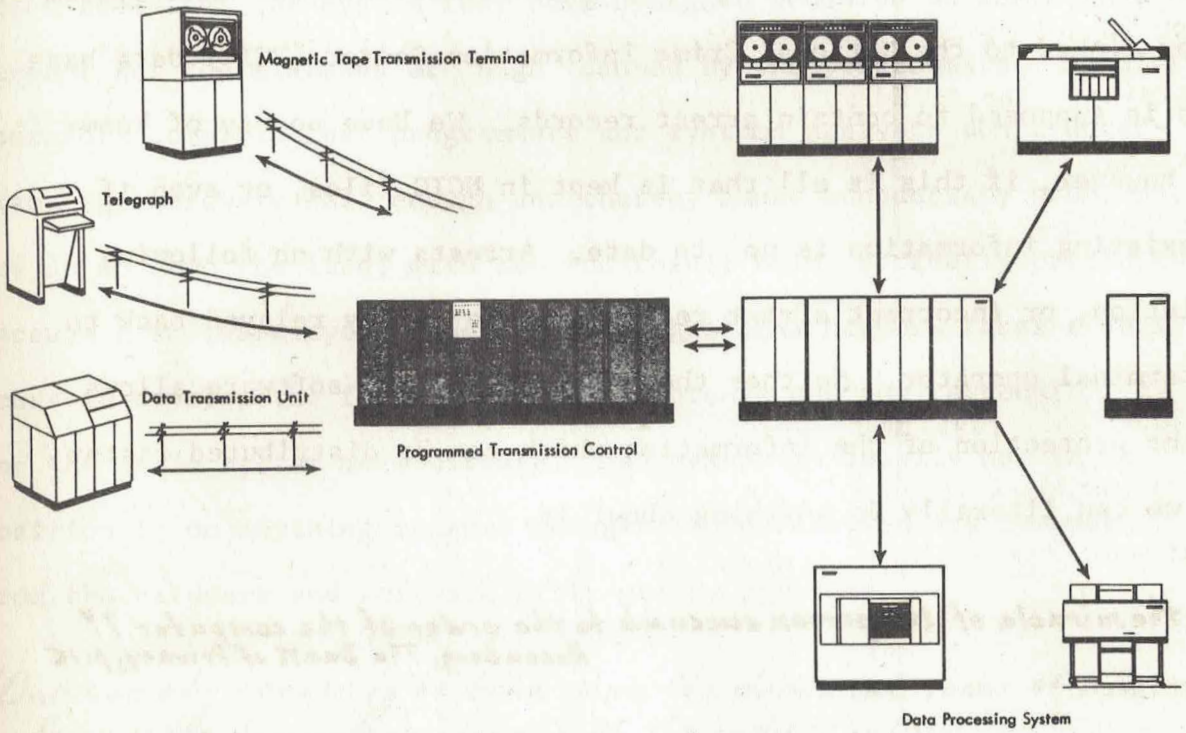
FEEDING THE BEAST

When the press refers to the "computer" they usually mean the equipment or hardware which is used to manipulate the data. Regardless of the size of the computer this hardware includes a core or memory device and several input/output devices which are used to store and transmit information.

An explanation of the threats which these "beasts" pose to privacy requires some understanding of the way in which they operate. The essence of computer functioning is the transformation of data from one form to another according to a previously supplied set of instructions. These instructions usually come more or less directly from a programmer, who is often drawn as the character responsible for "feeding" the machine.

During the past ten years the speed of both the input/output devices and the memory has grown enormously. A decade ago most commercial computer systems were essentially card systems, where keypunched cards

were read in and processed. Now higher speed devices like magnetic tape and disk packs can process and store information so rapidly that it almost seems that the computer is insatiable. One reel of magnetic tape for example, can hold more than 60,000 dossiers equivalent to the contents of about 100 books of 300 pages each. This whole mass of information can be processed in about ten minutes.



The mass of metal and wires pictured above is dependant on an army of computer workers to write the instructions (software) to make it tick. This diagram includes the hardware for a real time system which allows many terminals not necessarily located near the central equipment to use the data and programs stored at the main installation.

Real time systems are widely used by the airlines to keep track of reservations, but the techniques developed are easily adoptable to other types of data banks. Burroughs, for example, in conjunction with funds from the Law Enforcement Assistance Administration (LEAA) has designed

a real time police information system. Using this system a patrolman can call a license plate number to a terminal operator who will then query the central computer's data store (usually disk packs of information) about the owner of the registration.

The big question in the LEAA network, as well as the airlines, is what's in the central computer's bank of information. The LEAA system is now linked to the National Crime Information Center (NCIC) data base which is supposed to contain arrest records. We have no way of knowing, however, if this is all that is kept in NCIC files, or even if the existing information is up to date. Arrests with no following conviction, or incorrect arrest records can be easily relayed back to the terminal operator. Neither the hardware nor the software allows for the protection of the information which can be distributed faster than we can literally do anything about it.

"Must the miracle of the person succumb to the order of the computer?"
Rosenberg, The Death of Privacy, p. 15

ROLE OF THE PROGRAMMER

The computer industry has become increasingly compartmentalized into a hierarchy of worker categories, each with a specific job to do. Keypunch or terminal operators type information for further processing; machine operators mount the tape reels and disk packs as well as handle the processing procedures at the computer itself; programmers prepare the programs for the computer; and system analysts analyze and design the

computer programs necessary to make the system function.

Unfortunately, just as efficiency has left its mark on the job categories it has similarly left a residue on the division of responsibility between these classifications. Programmers for example, rarely see the data they are writing instructions about. Systems analysts often feel that the system they have designed would be perfect if it weren't for the mistakes or "bugs" caused by the programmers. Machine operators complain that programmers and systems analysts don't understand the hardware well enough and thereby cause unnecessary problems. And so on down the line, with the end result being perfectly predictable. Because a software system such as Burroughs LEAA network takes several years to develop the feuds become more intense and the responsibility for the whole system more diffuse. Management is usually not in a position to do anything because managers by definition are removed from the hardware and software nitty-gritty problems.

"Our society ceases to be free when the dominant focus of life becomes the technology instead of the individual..."
Rosenberg, The Death of Privacy, p. 15

The public is caught in this labyrinth with few alternatives. Obviously, we as citizens would like more of a say in the type of information compiled for computer use, and computer workers would like to have more control over the tasks they do, yet the industry has developed into a many headed monster where those that make the decisions and those that implement the work are divided from one another.

The Association of Computing Machinery (ACM), the largest organization in the field, has a set of guidelines which among other things call for a member to

> "...act in professional matters as a faithful agent or trustee for each employer OR client..." (emphasis is ours)

The organization makes no mention of the principle that the computer worker could or should be responsible to the public who are the ultimate users. The conflict between responsiblity to the public and alliance with a task group has, until recently, never been discussed in the industry. Individual workers who have made a fuss or refused to participate in a system with which they did not agree have often been fired, and their unemployed ranks are still growing.

MYTH OF TECHNICAL SAFEGUARDS

Many in the industry have begun to talk about technical or software safeguards which could be used to protect against theft or misuse of data. But the mere mention of technical safeguards is an indication that there is reason to believe that human safeguards have failed. Basically there are two kinds of data misuse, which can be characterized as wholesale and retail. Wholesale theft involves the possible divulging of large quantities of information, whereas retail abuse would include the threat of one or several individuals getting access to information for their own use. The wholesale abuses seem to be the most difficult to stop and the most effective weapons of repression.

An illustration of possible wholesale abuse might involve a company

or group of airlines which wanted to expand their data files to gain access to credit references or police data about persons reserving seats. The airlines are currently exchanging data with the FBI and other law enforcement agencies when requested to do so. Or suppose the companies decided to compile a personal dossier of the air miles logged by their customers. There are few choices for the computer workers who do not want to write the instructions. They could get together and fight the decision, but the saying "someone else will do it anyway" has some truth. They might decide to limit the uses of such a system by designing safeguards to allow distribution of information to only certain people, but this type of responsiblity falls far short of curtailing industry and government from keeping files on our behavior in the first place. Obviously, once the data is collected there is nothing to stop the Hoovers, Mitchells, and Nixons from using it.

The industry axiom seems to be that where human safeguards fail, technical stop-gap measures must be tried. These measures include code words for entry into a data system, security procedures around a computer installation, and programmed checks and balances in the computer software to "catch" unwanted modification of the data being processed. All of these safeguards are really aimed at the retail or small time crook who might be interested in picking up a few pieces of information. In accomplishing this type of protection, the technical safeguards can be moderately successful, but they in no way hinder government agencies and large corporations who want to exchange data.

EXISTING DATA BANKS

There are many different personal data banks that have been and are being compiled by both public and private organizations. The government's collection of data on its citizens is under the auspices of agencies like the Secret Service. The Congressional Record of December 15, 1969, quotes a guideline distributed by the Secret Service throughout the Executive Branch to encourage the reporting of information on people including those:

> "(who) have made threatening, irrational or abusive statements about or to government officials, ...(who) contact government officials for purpose of redress of imaginary grievances, ... (who would) seek to embarrass the President or other government leaders ..."

Who is to judge what is threatening, irrational, abusive, imaginary or embarrassing, or in light of government policies on war, racism and poverty, what ought to be so. The guideline also requested

> "information regarding anti-American or anti-U.S. Government demonstrations in the United States or overseas and information regarding civil disturbances."

This information has been requested in a country that has guaranteed its citizens free assembly.

Senator Sam Ervin in the same Congressional Record has stated that he "may qualify under the loosely written and even more loosely interpreted guideline the Secret Service has issued" as he is

> "a malcontent on many issues and has written the President and other high officials complaining of grievances that some may consider imaginary and, on occasion, he may also have embarrassed high government officials."

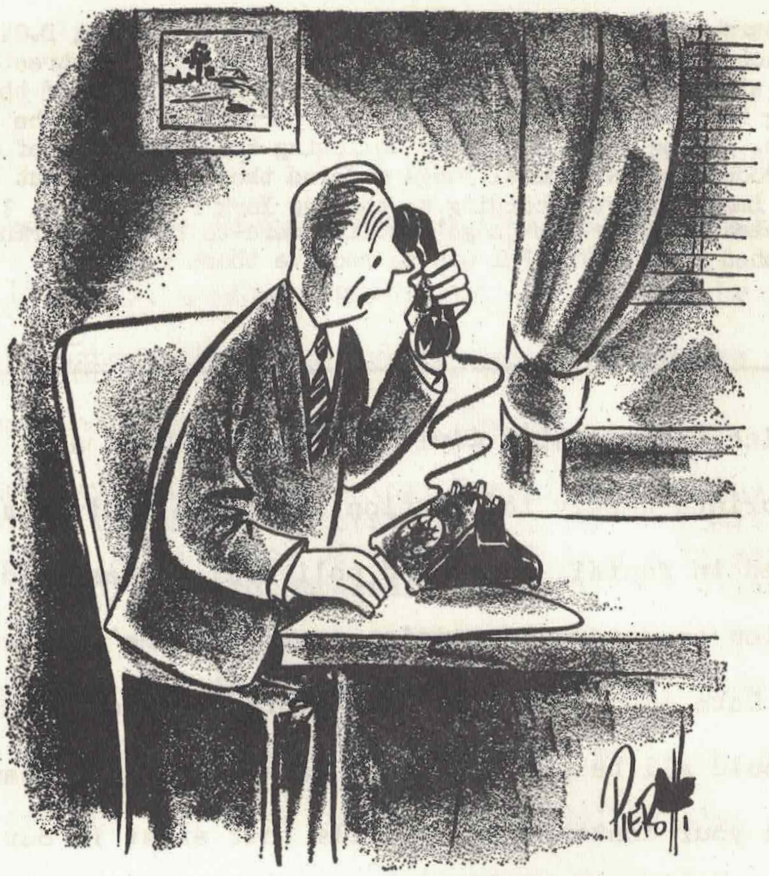
He and many others exercising their freedom of speech and free assembly now appear in a Secret Service data bank.

In the course of the Mayday demonstrations in Washington, D.C., over 12,000 people were arrested, many of them swept off the streets and detained without being charged with any violations. Many of them, according to press reports, had not been participating in the demonstrations. In the legal confusion following the suspension of normal arrest procedures, a Federal judge ordered those held without charge released immediately. According to the New York Post (May 5, 1971), "Those released under the judge's ruling were to be fingerprinted and photographed first." The FBI was to receive those records.

The Justice Department's Civil Disturbance Unit also compiles dossiers and prints weekly information sheets on individuals and groups involved in racial, class and political issues, and uses this information to determine tension spots and the militancy of its citizens. Data involving a welfare protest, union meeting or peace rally would all be put into this data bank. This means that if you express your contempt of the ills that exist in our society, your dossier becomes part of the Justice Department's data bank. Is not the purpose of a democracy to allow one to freely disagree with the government if one feels that it is necessary to do so?

The Department of Defense is also responsible for amassing dossiers on citizens. The Congressional Record of July 29, 1970, reprints a copy of a memorandum issued on March 6, 1970, by Stanley Resor, Secretary of the Army, to the Chief of Staff, which states:

> "In order to insure that no Army element in the United States is maintaining (a data bank system), I would appreciate your asking all commanders in CONUS, Alaska and Hawaii, down to the lowest level, to report whether their command has any form of computerized data bank relating to civilians or civilian activities, ...If a command has such a data bank, the data bank should be immediately destroyed unless a report justifying its existence is submitted for approval."



"HELLO, OPERATOR? FBI? U. S. ARMY?"

The Army was later embarrassed to discover that it maintained another data bank at Fort Hood, Texas. The Army had kept its operation so secret that it did not even know how extensive it was.

The Army has supposedly destroyed its tapes containing personal dossiers but its punched cards and programs probably still exist so the tapes could easily be recreated. Files are still being kept manually and, in his March 6 memorandum, Secretary Resor states that

the Army is "reviewing measures such as reductions in direct overt observations of incidents in progress, liason with local authorities and related spot reporting activities" which means that these activities were still being undertaken then, and probably still are now.

The Army is not the only member of the Department of Defense keeping surveillance reports on public activity. The Air Force's Bureau of Special Investigations publishes a secret bi-monthly bulletin "Significant Counter-intelligence Briefs". After the controversy over the Army data banks, it made an issue of the bulletin available to the New York Times. A high ranking DOD official said that the Bureau fulfilled its specific responsibility "of keeping commanders in the field fully informed" (Times, Jan. 29, 1971). The bulletin of January 6, 1971, contained in part; trends, U.S. activities (articles on "Anti-USAF efforts decrease in incidence and intensity" and "Huey Newton to abandon speaking campaign"), and notes on different geographic regions.

NYSIIS, the New York State Identification and Intelligence System, is a computerized data bank containing arrest, acquittal, conviction, and other related information on individuals arrested in New York State. NYSIIS is a typical state criminal data bank. Some states keep political surveillance files on citizens as well as criminal files in their data banks. In 1970 a number of workers in brokerage firms were fired for having arrest records. These included acquittal records and records of charges that were dropped.

> "A survey by the New York Civil Liberties Union indicated that 75% of New York area employment agencies would not accept for referral an applicant with an arrest record . . . . Another study of 75 employers indicated that 66 of them would not consider employing a man who had been arrested for assault and acquitted.
>
> "At the least, an arrest record is likely to lead to further investigation; and if it is convenient to fill the job before the investigation is complete, the applicant is effectively denied employment because of his record . . . . So long as there exists an employable pool of persons who have not been arrested, employers will find it cheaper to make an arrest an automatic disqualification for employment."
>
> — Chief Judge David L. Bazelon, U.S. Court of Appeals

The concept of "innocent until proven guilty" is abrogated by erroneous, out-dated and uninterpreted data contained in and distributed by such systems.

The Justice Department's Law Enforcement Assistance Administration (LEAA) was set up to administer grants to aid state law enforcement agencies in becoming more efficient in crime prevention. LEAA is acting as a coordinating body, tying together the separate state crime data banks with the FBI's National Crime Information Center (NCIC) on federal offenses. NCIC will enable anyone with access to any state data bank terminal to get the complete record of a person, not only from that state's data bank, but from NCIC and all other states tied in to the system. LEAA funding has been mainly for setting up computerized data banks by the states, and not only for criminal records; the Oklahoma Office of Inter-Agency Coordination was given an LEAA grant to maintain surveillance files on citizens.

The courts have occasionally upheld the right to freedom of speech and assembly without surveillance. In one such cases, New Jersey Superior Court Judge Robert Mathews ordered police dossiers destroyed, saying:

> "It is not difficult to imagine the reluctance of an individual to participate in any kind of protected conduct which seeks publically to express a particular or unpopular political or social view because of the fact that by doing so he might now have a record or because his wife, his family or his employer might also be included."

On June 1, 1970, the New Jersey Supreme Court overturned this decision and upheld the compiling of secret intelligence dossiers by the police.

In addition to data banks created strictly for surveillance purposes, there are many public and private data banks which exist for record-keeping but which are frequently used for surveillance purposes.

The Federal government invades privacy by its employment record-keeping. Some examples of questions asked on Federal employment forms, according to Senator Ervin (Congressional Record, March 8, 1970), are:

> I think the spread of birth control is essential to solving the world's economic and peace problems: Yes, uncertain or no.
> I am considered a liberal "dreamer" of new ways rather than a practical follower of well-tried ways: True, uncertain or false.

Such questions seem designed to keep employees in the government mold.

Another data bank of human behavior is the records of the Census Bureau. The 1970 Census has created the world's largest data bank. An individual has no choice by law as to whether he or she wishes to answer the countless personal, and often irrelevant, questions. Failure to complete the questionnaire is punishable by fine or

imprisonment.

The Census Bureau organizes its data into summary tapes, which consist of subdivisions of areas as small as city blocks, and sells these tapes to any buyers, private or public. No investigation is made by the Census Bureau as to the use of the information, and private summary processing centers give the bureau even less control over its information. A Census Bureau official has said that these private centers are "entirely on their own. We take no responsibility for their work."

The Census Bureau claims that there can be no invasion of privacy from its records since all data pertains to groups of people and not to individuals. Even apart, however, from the great temptation so much personal data must represent to Federal officials who in other ways constantly display their disregard for privacy, the possibility of violating this rule is created by the organization of the data into such small groups. Given some independently known information on individuals, dossiers on individuals could be extracted from some Census data. Agencies and individuals with access to Census data in addition to IRS, Social Security, HEW and other governmental "record-keeping" data banks, have the beginnings of the power to construct dossiers on everyone in the country.

Probably the largest private data bank is that of the Credit Bureaus. According to Hillel Black, the Associated Credit Bureaus of America have data on more persons than the FBI and CIA combined; approximately 110 million persons with more than seven million reports exchanged annually among members. (Rosenberg, The Death of Privacy)

These dossiers contain information such as employment history, salary, savings, loans, mortgages, other debts, legal proceedings. The Retail Credit Company has records on more than 45 million people with 35 million reports exchanged.

Errors can, and frequently do, occur on these files. Legal cases that were dismissed or settled continue to appear on file and have affected peoples' credit ratings permanently. Nonpayments may be reported or identified inaccurately. Correct or not, however, it still remains that information about an individual is made available to others without his or her knowledge or consent, often resulting in decisions or actions unfavorable to the person. The individual does not know what data is compiled about him or her, and if the information is found to be incorrect, it is very difficult to correct.

Credit agencies, which conduct their own surveillance of people and maintain their own record-keeping data banks, have also traded information with government agencies. The New York Credit Bureau, for example, has supplied data to the FBI and State Department.

"We must begin to learn what it means to live in a society that treats information as an economically desireable commodity and a source of power." Miller, The Assault on Privacy, p. 23

"There is a natural and close affinity between those who own the raw information about people and those who control the technology needed to manipulate and disseminate that information." Miller, The Assault on Privacy, p. 76

DATA BANK LEGISLATION

The law, like the question of technical responsibility, addresses itself primarily to the problem of distribution of information. There have been few attempts to stop the dilemma of data banking by stopping the collection of data.

The Freedom of Information Act in 1967 was probably the first major attempt to face the issue of the power of information versus the privacy of the individual. The theory behind the law was to give the public more control and better watchdog facilities by making many categories of "public" (governmental) data accessible by all the people. Unfortunately, in doing this, the law provided for the distribution of information at the expense of the people about whom the data is collected. While an individual seeking otherwise unavailable data can get a court order to retrieve information, there are no protections for the subject of the data.

In the commercial area, the Fair Credit Reporting Act, introduced in the Spring of 1969, jumped head first into the confusion of credit data abuses. The preamble to a draft of this bill stated, "An Act to enable consumers to protect themselves against arbitrary, erroneous, and malicious credit information".

Yet, just as the Freedom of Information Act started with lofty intentions and produced a mere whimper, the Credit Act approached much the same end. After many Senate and House dissecting sessions the bill was finally passed in 1971. Since the process of making laws requires a give and take by the forces that be, and since the large forces exert more take than give, the Credit Act does not begin to dent the power of the credit bureaus. It does, however, give an individual the right to access his or her own file, and the right to be advised when an adverse decision is made as a result of a credit report.

This last type of protection, the right of a person to be notified, has become the darling of the legislators trying to calm the mounting fear of privacy invasion. Needless to say it is a good idea, but places the emphasis for protection after the fact. The individual citizen will have to prove his or her innocence against the prosecution power of the large information collecting agencies.

DATA BANK TESTIMONY

The following position paper was submitted to Senator Ervin's hearings on Constitutional Rights.

I. The Computer and Civil Liberties

- COMPUTERS ARE A THREAT TO PRIVACY

As computer technicians, we in Computer People for Peace have the responsibility to inform the public of misuses and dangerous applications of computers. As citizens we fully understand the public's fear of computers and feel that much of that fear is well-grounded in the threats to privacy presented by the speedier distribution of information made possible by technology.

- THERE ARE NO TECHNICAL SAFEGUARDS

Because we work in the computer field we know that there are no software or hardware constraints which can be incorporated in any system to make it foolproof. All technical safeguards built into computer systems such as keywords, scrambled indexing and limited access, must be designed and implemented by people, and therefore may be "cracked" or decoded by others with an interest to do so.

In no way could we abdicate our responsibility to the public by making them believe that we could technically design data bank systems which could offer them the protections they need. The solution must rest with the people and the enforcement mechanisms they devise; it cannot rest in the computer industry, although the industry must take responsibility for its actions.

- RESPONSIBILITY OF DATA REQUIRED

Some have suggested that in order to secure more controllable computer systems, programmers and other systems personnel be licensed. We have seen that the Army and its data processing staff, which is well-controlled and under security clearance, has violated our rights. Who is to license those who license? We do not believe that licensing in any way purifies or isolates the problem of data banks. We do feel, however, that the problem should be tackled from the standpoint of "responsibility of data". In government as well as private industry, an individual or group of individuals in charge of a project should be held accountable in a court of law for violations of our rights of privacy.

- OBLIGATION OF TECHNICIANS TO THE PUBLIC

The computer field, which has led the way in efficiency methods, has intensified the issue of dehumanization. Many of us who are programmers, operators and systems analysts know little if anything about the end product or value of our work. As citizens we feel that we must have more of a say in the type of work we do. As technicians we feel that it is imperative that our responsibility be to the public, not to our corporate employers.

II. The Government and Civil Liberties

- BILL OF RIGHTS MUST BE ENFORCED

The computer has brought the problem of data banks and individual privacy to a head, but it is in no way the sole culprit. The computer makes it easier to collect and distribute information at speeds which were a few years ago inconceivable. It is therefore necessary for the people to insure protection from their government by more rigorously enforcing the Bill of Rights.

Although this document was written almost two hundred years ago it offers concepts which are still viable. The First and Fourth Amendments explicitly grant us the right of personal privacy. Data accumulated about a citizen must fall under the same safeguards as the rights of the citizens themselves.

- THE GOVERNMENT HAS VIOLATED ITS OWN LAWS

Given a government which has frequently violated its own laws (as shown by the Army intelligence operations, the passport lists, and other data banks brought out in the Senate hearings), it is not more laws that we seek, but enforcement of existing safeguards.

We need not be legal experts to see that additional laws can only muddle the thinking of the Bill of Rights which contains all the information we need to solve this problem. The "freedom of Information Act" attempted to define "public information" to benefit the people. In practice, however, it has become an example of the infringement of additional laws on our basic rights. Through this act, many agencies have justified continuing a policy of selling information (such as census data) under what we believe to be the misguided concept that information can be sold to the public for money.

Information about an individual should be considered his or her own property and be available to others only upon release by the person involved. In no way should dollar values be attached to the invasion of an individual's privacy.

- PEOPLES RESEARCH BODY NEEDED

In order to enforce our rights more rigorously, we think it necessary to create a People's Research Body. This body should be composed of individuals from consumer interest organizations, legal rights groups, citizens interest committees and workers from the computer field. It should remain apart from the government so that it may involve itself in objective research into infractions of our rights of privacy by the government. The research performed by this body should result in indictments which can then be brought before a court of law.

In the past we have seen regulatory agencies grow into bureaucratic nightmares, resulting in the creation of more problems than they solve. In order to avoid this tendency, we urge that the People's Research Body be limited in power and composed of lay citizens who will serve in terms of no more than one year, selected in a manner similar to jury service.

- DATA DISARMAMENT TEAMS NECESSARY

In addition Data Disarmament Teams should be established to follow up court-mandated destruction of existing data banks. In instances in the past, like the Fort Holabird files, court-mandated destruction of data banks has resulted in the erasure of computer tape files while the original input data on computer keypunch cards was maintained.

- INDICTMENTS MUST BE BROUGHT

We fully realize that our suggestions place a great deal of faith in an already overworked and often inconsistent judiciary system. We must accept this as an interim measure. The government must give us a sign of faith by proving that it is serious about our rights. Indictments must be brought against those responsible for the present course of action. We feel that the maintenance of data banks like the Army data banks and the NYSIIS system constitute a conspiracy by the government to deprive the people of their constitutional rights to privacy.

We enthusiastically support legal cases now being brought against the government by individuals and groups concerned with our privacy. We urge the judiciary to respond with a clear understanding of the dangers of technology and a strict interpretation of the Bill of Rights.

III. Criteria for the Right to Privacy

If the judiciary does its job, we believe that the Bill of Rights provides sufficient protection for the people from the government and from corporate incursions on the right of privacy. The following specific protections should come under the scope of the Bill of Rights if it is interpreted correctly. If, however, the judiciary fails to fulfill its obligations, further steps by the people may be required to guarantee the right of privacy of information by instituting protections like the following criteria.

1. The concept of "public information" as currently defined needs to be restricted along the lines of "name, address and social security number". Arrest and conviction records, school records and other personal history information should not be made public information.

2. There should be no transfer of data from one agency to another and no sale of information under any circumstances.

3. Individuals should be informed by periodic audit notices of all information about them held on any data bank, private or public, and should have the power to have any such data altered or destroyed beyond the data defined in (1) above.

4. No person should be denied any public or private service, right or employment opportunity for refusal to supply personal data beyond that defined in (1) above.

5. All questionnaires seeking personal data should carry a printed explanation of what information a person is obliged to supply for the purpose of the questionnaire.

6. The substance of all legislation and regulations should establish a criterion of "need to know" for the collection of any data on individuals and the burden of proof of this need should rest with the collecting agency.

7. Statistical data necessary for analysis and planning by public and private agencies should be collected in such a way that none of it can be traced to any individual.

8. Retention cycles should be established for the maintenance of all data collected on individuals.

"Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent, information about them is communicated to others." Alan Westin

SUGGESTED READINGS

Computerworld, a weekly trade newspaper. 797 Washington St., Newton, Mass. 02160

Gallagher Report, The computer and the invasion of privacy--hearings before a subcommitte on Government Operations, House of Reps., 89th Congress, Second Session, U.S. Government Printing Office Washington, D. C. July, 1966.

Hoffman, L. J., Computers and Privacy: a Survey, Computing Surveys, Vol. 1, No. 2, June, 1969.

Miller, A. R., The Assault on Privacy: Computer, Data Banks and Dossiers. The University of Michigan Press, 1971.
this book is an excellent and extensive report on data banks.

U. S. Congress, Privacy and the National Data Bank Concept, House Committee on Government Operations, US Government Printing Office, Wash. D. C., August 2, 1968.

Westin, A. F., Privacy and Freedom, Atheneum, New York, 1967.
this book contains a good bibliography.

Forthcoming--Transcript of Sen. Ervin's Subcommittee on Constitutional Rights, write US Government Printing Office.

ABOUT CPP

This booklet was written by the Data Bank Collective of Computer People for Peace. Although it is primarily intended as a survey for those not in the computer field, we hope that it presents an overview for computer people who are concerned with attacking the problem on their jobs.

Computer People for Peace was started more than 3 years ago around the issue of the War in Vietnam. Now, like many groups, we are bringing our focus on the related problems here at home. We feel that the work we make computers do is at best meaningless, at worst it is lethal.

For further information, or additional copies of this booklet please write to:

CPP

Enclosed is ____ for ____ copies of DATA BANKS, PRIVACY AND REPRESSION @ 50 ¢ each.

☐ Please bill me.

NAME _____

ADDRESS _____

_____

☐ Please put me on your mailing list.

Write for bulk rates for 10 or more copies.

COMPUTER PEOPLE FOR PEACE
THE DOLPHIN CENTER
137A WEST 14th STREET
NEW YORK, N. Y. 10011