LDIR#012

CRIMINAL JUSTICE AND RIGHT OF PRIVACY 2 FED. DEPT. AGENCIES AND REPORTS 1970-1972

The Washington Merry-Go-Round

By Jack Anderson

WASHINGTON--Many Americans do not realize their privacy is being invaded by the Retail Credit Company, a private snooping agency that has collected files on more than 45 million American families.

With a network of over 300 branch offices in the United States, Canada and Mexico and a staff of over 7,000 inspectors, Retail Credit probes into the intimate aspects of a person's life

Then it churns out a report, which may be inaccurate but can nevertheless determine whether the unsuspecting person will get a job, insurance or credit.

Congressional investigations have not dampened retail credit enthusiasm for playing surveillance games and selling their findings to insurance companies, credit card firms, retail businesses and other clients.

Lately, however, the Oklahoma Attorney General's office, the Federal Trade Commission (FTC) and Ralph Nadar have been studying Retail Credit's practices.

In Oklahoma there is an enlightened statute which is strangely missing even in states with consumer-oriented reputations. It requires anyone about to submit a credit report to a retail business concern to first send a copy to the person involved.

Retail Credit, in some states at least, has also allegedly violated that part of the new federal Fair Credit Reporting Act which requires them and other private credit snoopers to let people find out what information is in their credit file.

TABLES TURNED

Now we have turned the tables on Retail Credit and have done some investigating of our own.

Insiders slipped us the company's private "Inspector Manual," their "Manager Manual" and the forms used by Retail Credit inspectors in their day-to-day rounds.

We have also collected data from those who are in Retail Credit's files, spoken with Retail Credit's workers, and even run a test on material in Retail Credit's fles on us. These are the results of our investigation:

We find hard-pressed inspectors are often assigned a daily caseload of from 10 to 15 people to investigate, hardly an encouragement for painstaking reporting.

If a health or life insurance applicant is being investigated, the inspector will delve into that person's finances, occupation, driving record, hobbies, health, drinking habits, family environment and reputation, including home, social and club life.

The inspector's method usually is the "neighborhood check" which means most of the information acollected is obtained from neighbors who now the person being investigated and are willing to talk, but who may provide false and malicious gossip.

H. E. Nichols, vice president in charge of public affairs for Retail Credit told Gay Cook, my investigator, that, "Inspectors make every possible effort to interview the person being investigated."

DO, BUT DON'T

We found, however, that some Retail Credit inspectors make little or no effort to reach those being investigated. The Inspector Manual bears us out, stating plainly that inspectors should "endeavor to investigate in such a manner that the applicant or insured will not learn of the investigation."

Retail Credit also instructs its inspectors to come up with a "quota" of protective--that is averse--information on the hapless citizen. In fact, inspectors must fill out a daily form showing just how much protective information they have culled.

They must also report the percentage of cases in which they recommend denial of an applicant's bid for a job, insurance or a credit rating.

This appears inconsistent with the Fair Credit Reporting Act's demand for accurate reporting because it tends to put pressure on the inspector to write adverse reports.

Retail Credit also has a bonus plan to drive the inspectors to even greater production.

The major injustice to the consumer is that the consumer is that the Fair Credit Reporting Act dos not compel Retail Credit to let you examine your own file or to divulge medical information they have collected.

Footnote: When one of my reporters called Retail Credit in Washington they courteously readhimhisfileafterverifyinghisid errors which were corrected on the spot: one, the number of cars he owned; two, it had him once working at the wrong job; three, it listed his deceased father as living. Although the errors weren't serious, if they had been made on finances, health or drinking habits it could have destroyed his chances for a job, insurance or a good credit rating. The most frightening aspect of the file was how much correct information Retail Credit had discovered about his income, health, appearance, relationship with his family, traffic record and financial condition.

SOUTHEAST ALASKA EMPIRE

AN INDEPENDENT NEWSPAPER
Published daily, Monday through Friday (except holidays) by Southeastern Newspapers Corporation, in the Southeast Alaska Empire Building, 130 Nicla St., Juneau, Alaska 99801
Second Class Postage Paid at Juneau, Ak.
TELEPHONES
All Departments [illegible]
Subscription Service [illegible]
Member of the AP wire and NEA news services. Represented for national advertising by Nelson Roberts and Associates, Inc., 410 First Avenue West, Seattle, Washington 98119. Phone ATwater 4-[illegible]
HOME DELIVERY RATES
One Month $1.75
One Year $18.00
MAIL SUBSCRIPTION RATES
(Payable in Advance Only)
INSIDE ALASKA
$3.10
OUTSIDE ALASKA
$3.50
AIR MAIL
$7.25

8-10-71

he Right of Privacy

ITH 1971 has come increasing recognition of the individual ht of privacy, but also the tech- ogical means to invade—possibly nullify—that right.

The technology developed to cure ills of civilized men has created its n social problem—"the painfully iiliar problem of a technology that s outstripped our knowledge of how use and control it."

This problem that Yale law profes- r Joseph W. Bishop, Jr. saw in re- nciling privacy rights with the use electronic surveillance in criminal ses, is equally relevant for the wide- read private and public information- thering recently revealed during arings of the Senate Subcommittee Constitutional Rights.

In the name of "efficiency" and "se- rity"—an excuse for legal wiretap- ıg already challenged in U.S. federal urt in California for its broad appli- tion to cases of domestic organiza- ns suspected of subversive acti- ies—the federal government has un a web of surveillance activities it threaten not only our con- tutional right of privacy but free litical expression itself.

One civilian target of Army in- lligence, Senator Adlai Stevenson III).-Ill.) railed: "Spying and snooping d data banks profits no one—except revolutionaries. It lends credence their charges that ours has become unjust and repressive society."

Whether the hackneyed spectre of g Brother is looming over the nerican public may yet be a pre- ature question. Nevertheless, can we ıore the threat of a government med to the hilt with "unforgetting" mputers, declaring data banks the nacea of effective law enforcement, d using sweeping non-guidelines to strict what information is finally col- cted and processed?

The Justice Department firmly de- nds its right to engage in widespread rveillance—usually coordinated with e Federal Bureau of Investigation ıd the Secret Service, not to mention ate and local law enforcement gencies whose intelligence capabilities ıve been enormously fostered rough grants from the Justice De- rtment's Law Enforcement Assist- ıce Administration.

Assistant Attorney General William . Rehnquist of the Office of Legal Counsel, told the subcommittee:

"We believe that full utilization of advanced data processing techniques is by no means inconsistent with the preservation of personal privacy.

". . . I think it quite likely that self-discipline on the part of the Executive branch will provide an answer to virtually all of the legitimate complaints against excesses of information gathering.

". . . The Department will vigorously oppose any legislation which, whether by opening the door to unnecessary and unmanageable judicial supervision of such activities or otherwise, would effectively impair this extraordinarily important function of the federal government," Rehnquist maintained.

While the Justice Department would skirt any real limitation in exploiting its full law enforcement powers, Secretary Elliot L. Richardson of the Department of Health, Education and Welfare sees the potential danger inherent in indiscriminate information gathering. Testifying about his department's confidential Social Security data banks, Secretary Richardson pointed out:

"The potential for invasion of privacy or breach of confidentiality of information lies not in the use of the number itself, but rather in how the organization uses computerized collections of data which are indexed by the number."

". . . Government," he added, "is not the owner of information on individuals but only the *trustee*. As trustee, it must honor its fiduciary responsibility, using the information for the benefit of society and in the manner authorized by its individual owner."

At issue, then, is the question of control of the data, and the individual's complete ignorance of who is watching, what they are seeing and how that information once compiled will be used.

The computer has put special stress on a society devoted both to science and liberty. In expanding our knowledge, and capacity for knowledge, it is also capable of producing a terrorizing state of information overkill.

As Senator Charles Mathias, Jr. (R.-Md.) noted: "If knowledge is power, this encyclopedic knowledge gives the government the raw materials of tyranny."

Proliferating articles and books alert the average citizen to the dossiers upon dossiers marking his life from infancy through adulthood, following him everywhere he goes, and threatening to undermine his next job application or credit rating. Paranoia—haunting and real—pervades the land, as each new disclosure widens the known data base.

But Dr. Alan F. Westin, Columbia University professor of law and government and director of a National Science Foundation study on the political implications of data bank files, refutes Ralph Nader's warning that the computer will turn us into "a nation of slaves."

"The right to be let alone is the right most valued by civilized men."

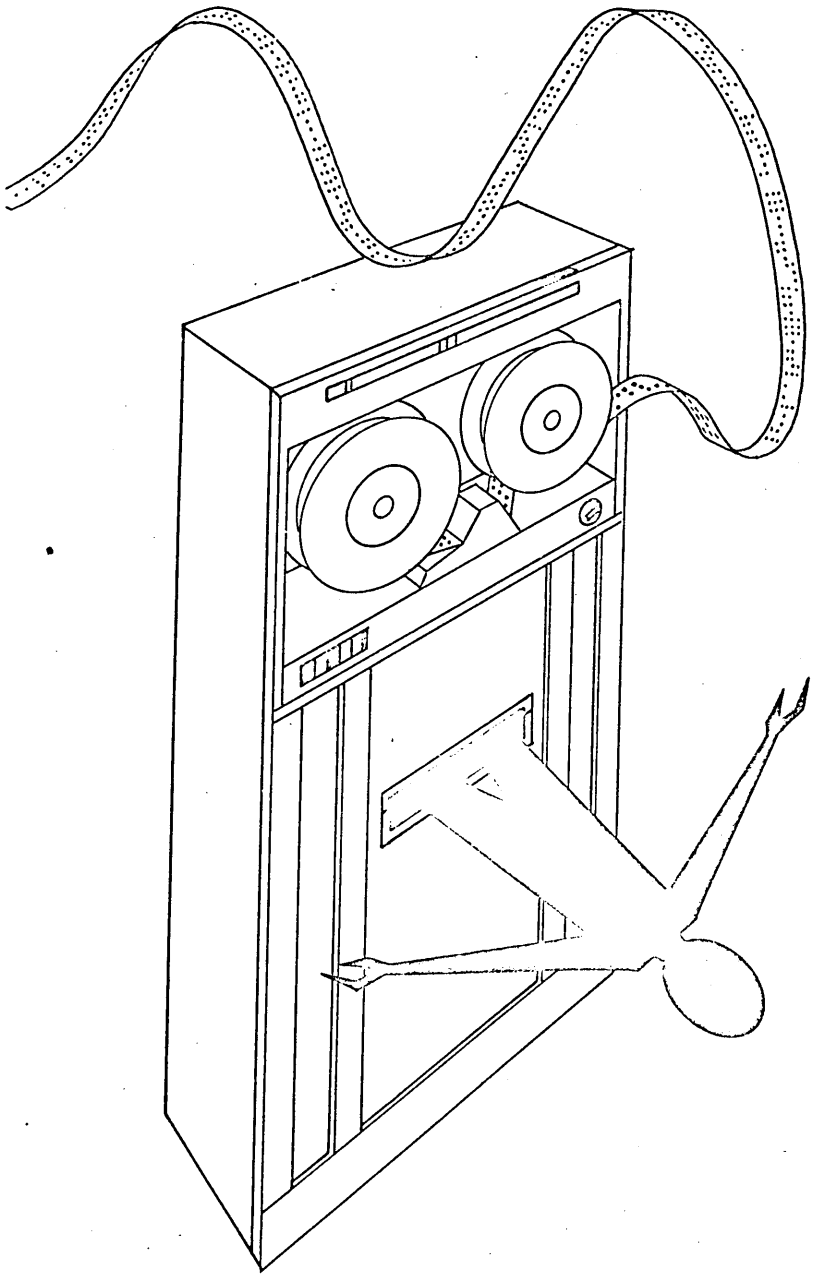
—Justice Louis D. Brandeis, 1928

Westin maintains: the very computers that threaten constitutional freedoms can be programed, with slight alterations, to provide better protection of privacy and individual rights than existed before the electronic age. They could discard and erase all criminal records after five years of good conduct or make it impossible to get out of computer storage a piece of information without generating a record that someone has asked for that information, and who has asked and why.

"Computers," he added, "even make it possible to have direct, automatic notification to the subjects, themselves, that their records have been opened and queried."

The security-privacy controversy demands full and fair discussion. Yet efforts to weigh the benefits of a comprehensive surveillance system—in fighting our exploding crime rate, for instance—against the potential dangers of the computer's ubiquity often encounter reluctance on the part of surveillance proponents to enter debate. Does this silence of the Defense and Justice Departments represent the courage of conviction, not to be daunted in the full exercise of their law enforcement powers, or a political reaction to civil libertarians and strict constructionists alike who challenge the extent of those powers in this uncontrolled sphere?

In any case, TRIAL asks: Are not controls evidently necessary when the use, misuse, overuse and abuse of data collected to safeguard democracy could conflict with basic democratic ideals upon which our country is founded? □



But these new devices have accorded those who control government increased power to discover and record immutably the activities, thoughts and philosophy of an individual at any given moment of his life.

The government can now take note of anything, whether it be right or wrong, relevant or not, and retain it forever. Every person's past becomes an inescapable part of his present and future.

The computer never forgets.

The new technology has made it literally impossible for a man to start again in our society. It has removed the quality of mercy from our institutions by making it impossible to forget, to forgive, to understand, to tolerate. When it is used to intimidate and to inhibit the individual in his freedom of movement, associations, or expression of ideas within the law, the new technology provides the means for the worst sort of tyranny. Those who so misuse it to augment their own power break faith with those founders of our Constitution who, like Thomas Jefferson, swore upon the altar of God eternal hostility against every form of tyranny over the mind of man.

These developments are particularly significant in their effect on the first amendment to our Constitution.

No longer can a man march with a sign down Pennsylvania Avenue and then return to his hometown, his identity forgotten, if not his cause.

No longer does the memory of the authorship of a political article fade as the pages of his rhetoric yellow and crumble with time.

No longer are the flamboyant words exchanged in debate allowed to echo into the past and lose their relevance with the issue of the moment which prompted them.

No longer can a man be assured of his enjoyment of the harvest of wisdom and maturity which comes with age, when the indiscretions of youth, if noticed at all, are spread about in forgotten file cabinets in basement archives.

Instead, today, his activities are recorded in computers or data banks, or if not, they may well be a part of a great investigative index.

Some examples come readily to mind:

• **The Civil Service Commission** maintains a "security file" in electrically powered rotary cabinets containing 2,-120,000 index cards. These bear lead information relating to possible questions of suitability involving loyalty and subservice 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 Commssion has found it a reasonable, economical and invaluable tool in meeting its investigative responsibilities. It is useful to all federal agencies as an important source of information.

the final answer: The People in Control

by U.S. Senator Sam J. Ervin, Jr., (D.-N.C.), Chairman Senate Subcommittee on Constitutional Rights

MODERN TECHNOLOGY has created unique resources capable of defeating at will the constitutional principles on which our freedoms are based.

Through the development of computers, data banks and telecommunications systems, government now has the means to satisfy easily its boundless curiosity about private citizens.

To be sure, recordkeeping is nothing new in the history of government; nor, indeed, is the habit all governments and all societies have of surveillance, blacklisting and subtle reprisal for unpopular poitical or social views.

Men have always had to contend with the memories of other men.

Out with

CHARLIE GREEN isn't his real name. But Charlie's problem is real. He has been living with it since 1962. Yet he didn't know what his problem was until five years later, and now, some nine years since, he still has not licked it.

What really hurts is this: it wasn't Charlie's fault that erroneous information got into a character credit report on him.

Charlie Green's privacy was shattered, and it nearly shattered his life. It has cost him money in lost income and attorney's fees.

His tragic story came out in the May 1969 hearings before my Subcommittee on Consumer Credit Institutions, from which developed the Fair Credit Reporting Act, signed into law and effective April 25, 1971. Professor Alan F. Westin, director of the Center in American Liberties, Columbia University, told Charlie's story, which was corroborated by Bernard McHeard of the Senate committee's staff. Westin chose the pseudonym Charlie Green to protect the real man.

After graduating from an eastern university in the early 1950s, Charlie Green spent three years in the Army, worked for a management consulting firm, then settled down behind a desk in a large insurance company.

He married and began raising a family. After four years, he went into sales work with an equipment manufacturer, but because of a merger, he was soon out of a job. Good recommendations, however, plus an unprecedented high score on a six-hour diagnostic and aptitude test landed him a job with a large national manufacturer.

All seemed right with Charlie Green.

About a week after starting, however, his sales manager called him into his office and accused Charlie of lying about some important information on his application form. He had not lied, Charlie averred, and if the sales manager would tell him what the matter was he could clear it up.

The manager said he "couldn't reveal the information" and that Charlie should "come clean." Charlie could not, of course, for he had not lied.

The sales manager grew cold toward Charlie. Charlie found working conditions intolerable and finally resigned.

He applied to many big firms, but just when it looked as if he had a job, he would be given the cold shoulder and the job slipped away. Even after he found work with a smaller company at less pay, he kept applying to bigger firms, always without success, always without a clean-cut explanation as to why he was not hired.

In 1967 the personnel manager of a national consumer product firm inadvertently told Charlie he failed to pass a pre-employment investigative check.

"I just can't hire you," the personnel manager said. "I don't think any company in the industry will hire you with that report."

"What kind of report?" Charlie asked.

He wasn't told. The manager said: "I really shouldn't have said what I did and I just can't tell you any more."

"I felt an absolute trembling fear for my family and myself," Charlie later told Westin. "What was I accused of? How was this situation ever to be resolved?"

Charlie learned that one firm did most of the pre-employment investigations in his field. A friend agreed to obtain a report on him just as if he had applied for a job with his (the friend's) company. Charlie finally saw the report in September 1967—five years later.

He "passed" the sections labeled "Employment-Educational Record," "Finances" and "Legal Record." But under "Reputation" were these nightmarish items:

- "Said to have been dishonorably discharged from the Army."
- While living in an apartment in 1961, a lonely woman neighbor complained about a noisy party in Charlie's apartment, called the police. After the police left, the woman said Charlie and his wife came to her apartment, cursed her and spit in her face.
- The landlord said he was glad when Charlie moved.

The facts were these:

Charlie had an honorable discharge papers. The neighbor woman was a recognized pest and several persons had moved from the apartment building because of her. Charlie had not done the things he was accused of doing. In fact, Charlie and his wife had brought suit to restrain the woman from harrassment. The woman filed a cross suit. But both suits were withdrawn at the suggestion of a judge and both attorneys.

- The landlord gave Charlie a letter saying he and his wife had been perfectly satisfactory tenants.

The astonishing aspect of the pre-employment investigative report—the original and all the subsequent ones—was that it dealt only with the year 1961. There was nothing about his reputation for years since then, and apparently no attempts were made to check Army records, to talk to anyone other than the complaining neighbor—not even the landlord.

Charlie's report was made by one of the most reputable firms in the credit investigative business!

"All I want them to do is clear my name, to show me a clean report and to tell me which (would-be) employers received derogatory reports," Charlie said recently. "They refused to do that on a negotiated basis so I had to sue."

His suit for damages is still unsettled. As Charlie says, his experience is a crime against society.

Had Charlie Green's demoralizing experience been an exception we might be able to "tsk," "tsk," it away. But the Senate subcommittee hearings showed it was not an exception; abuses occur often enough to have required legislation.

Had the new law been in effect in 1962, Charlie could have quickly cleared himself for it provides, among other protections, that a person turned down for credit, insurance or employment because of an unfavorable credit report be informed of that along with the name and address of the reporting agency.

With the rapid computerization of the credit reporting industry the chances increase for erroneous reports. Cases similar to Charlie Green's could multiply, although, because of the new law, perhaps they will not be as protracted.

There is a maxim in cybernetics: garbage in, garbage out. If errors are fed into computers, errors will be in the print-outs.

Ask any of the hundreds of persons who have written me complaining about billing errors made by computers. There is a lot of garbage to be kept out of the computers. Computers storing buying and bill-paying information cause enough inconvenience. Computers storing bits of private information about millions of consumers in this country can—and do—cause personal tragedies.

How extensive is the use of computers by credit bureaus and other credit reporting agencies?

Society's threat: The Military Sleuth

by U.S. Representative Abner J. Mikva (D.-Ill.)

WE SEE MOVIES like "Seven Days in May," "Z," and those about Hitler's Germany in World War II, and we smugly congratulate ourselves that none of this could happen in our beloved country.

Except that it could be happening right now. Right now someone could be tapping your telephone, screening your mail, watching your family or your office staff or your public officials.

A funny thing happened to *me* on the way to preparing this article. I found out I was sharing my privacy with the Army. The first trickle of information about the Army's pernicious practice began to leak out of the vast military bureaucracy late in 1969. Christopher Pyle, a former Army intelligence officer, wrote a long, detailed and thoroughly documented article for the *Washington Monthly* magazine describing the widespread use of undercover agents by Army intelligence to monitor civilian political activities.

Although various excuses and justifications were offered, it was clear from the beginning there was absolutely no sanction, either in law or in the traditions of this nation, for this kind of military snooping. Pyle's disclosures were followed finally by promises to cease further secret spying on civilians and to destroy existing files on domestic political activities. The sincerity of these promises may be judged from events in the ensuing months.

In December an NBC Special Report revealed that secret military agents had actually been present on the floor of the Republican and Democratic conventions in Miami and Chicago. This revelation, too, was followed by a spate of denials from high-level civilian officials in the Department of Defense that any such activities by military personnel had been authorized.

This left two possibilities: either these high-level civilian officials were being deceived by their subordinates about the nature and extent of military spying, or these officials were willfully misrepresenting the existence of authorized military spying. In either case, some investigation should have been conducted. Apparently, none ever was.

That report convinced former Army intelligence agent in Chicago, John M. O'Brien, to come forward with his hair-raising story of Army surveillance of civilian politics and elected public officials. Mr. O'Brien has responded to a higher kind of patriotism, a patriotism which requires citizens to speak out against the illegal usurpations of their government.

John O'Brien's revelations have profoundly shocked the people of Illinois and the people of this nation. What those revelations made plain is that military authorities have not limited themselves to surveillance of alleged "radicals" or violent demonstrators. The Army high command has decided that even elected officials—the very establishment itself, if you will—contain among their ranks persons who must be "watched," or whose activities must be "monitored."

Among those untrustworthy souls who needed these special attentions were a candidate for the U.S. Senate, a sitting member of the House of Representatives, a former governor of Illinois and present member of the U.S. Court of Appeals for the 7th Circuit, and at least two members of the Chicago City Council. In addition, they were watching lawyers, newspapermen, television newscasters, teachers, philanthropists, and Republicans. They even made sure that there was no racial discrimination in the surveillance and included civil rights leaders and other black citizens.

What were the criteria for such surveillance? According to Mr. O'Brien, they were people who were outspoken against the war, people who belonged to peace organizations, people who criticized the President on matters either foreign or domestic. In short, it aimed at active citizens.

The implication of the O'Brien disclosures and those which preceded them are overwhelming. How many candidates for Congress, for governor, for mayor, for city council, for state legislature, for any public office, have been subjected to this unworthy scrutiny? How many private citizens will in future years be deterred from participating in the political process—the lifeblood of a free society—by fears of military intervention, of having their children and wives watched.

Many have called John O'Brien's revelations "incredible." Yes, it strains one's credulity, but I believe that we can ignore these charges only at our peril if we wish to remain a free country. I would remind my colleagues that reports of the My Lai massacre were also first labeled "incredible," that only after a thorough, prolonged probe of the incident were the true facts brought to light.

But why does military surveillance of civilian politics endanger the kind of free society which we believe exists in America? It seems improbable that one should have to enumerate the reasons, but apparently there are those in government and in the military who do not understand the dangers.

First, of course, is the danger that surveillance—or even the popular belief that it exists—will discourage the kind of full, free, and unrestrained exchange of ideas and viewpoints on which democracy is based. When citizens and participants in political debate feel that they must restrain their utterances, that they must watch their tongues, because "someone might be watching," then we have taken the first step toward totalitarianism. It has long been the hallmark of totalitarian societies—police states—that only "approved" persons could participate and only "acceptable" ideas could be heard. Military surveillance of civilian politics raises the specter of such official "approval" and "acceptability" as some day being a requirement of American politics.

Indeed, those military officials who would arrogate to themselves the duty to watch peaceful civilians' political activities are the true subversives in our society. It is they who, more than critics of the Viet Nam war, pose a threat to the continued freedom of political expression and political action. They have betrayed the trust of the American people. They have betrayed their oath of office.

Military officials who have misused their authority to spy upon civilian officials to whom they are constitutionally responsible will in the long run do far more damage to our constitutional form of government than all the dissenters and critics put together. For who will protect us when our protectors pervert their constitutional function and turn their authority against the citizens they are pledged to serve?

The second danger from military surveillance of civilian public officials is the possibility that the existence of such activities, or even the belief among public officials that it exists, will influence the decisions which these officials are bound by oath to make on the basis of the public interest alone.

This subtle but very real form of intimidation has undoubtedly already begun to work. From jokes among legis-

Crime's Panacea

y Richard W. Velde, Associate Administrator
aw Enforcement Assistance Administration

UR POLICE, courts and correctional agencies have always maintained criminal information and intelligence files o do a better job of apprehending suspects, protecting the nocent, passing equitable sentences on offenders, selecting e proper rehabilitation for an offender, and, of course, cating stolen property and automobiles. A most serious eficiency throughout the criminal justice system is the reat lack of reliable and timely information.

Computerized information systems represent a basic emedy. *Operationally*, they can provide quick access to riminal histories vitally needed in the day-to-day operations of the criminal justice system.

Police need information when they have detained a susect, when they are trying to determine probable cause to rrest, and after having made an arrest.

With quick access to criminal information, a judge or agistrate can make a much sounder decision on whether o grant bail, or whether to sentence a person to prison or lace him on probation, or recommend special treatment.

Correctional agencies can benefit in making critical decions about methods of treatment, parole and work reease—decisions often made without the appropriate facts.

From another operational standpoint, information systems can assist police in pinpointing the frequency and ocation of crimes and the times they are most likely to ccur. Thus, police can more effectively assign manower—adding men to the critical shifts and supplementig patrol in high crime areas.

Information systems are also valuable as a source of verall information to evaluate and improve the criminal stice system—that is, in compiling complete, meaningful tatistics within the parts of the system, within metropoliin areas, within states and, ultimately, nationwide.

The effectiveness of the criminal justice system cannot be auged accurately without knowing what actually happens o people brought into the system. How many tried are onvicted? How long did they wait to go on trial Are they eleased before trial? Are sentences uniform? What is the ate of recidivism?

In its efforts to fashion a safer society, the Law Enforcement Assistance Administration has funded various actities in the criminal justice information field:

- Project SEARCH—a cooperative venture among ten tates with sights on a central nationwide index whereby a uery (with perhaps no more information than an license umber) would uncover whether a file existed on an indidual, give a brief summary and tell what state kept the ull record. A second inquiry to the state of record would roduce the detailed criminal history.

Project SEARCH has also successfully developed and emonstrated a new statistical series—offender-based transction statistics—which will enable planners and managers o have a comprehensive and timely factual data base on he dynamics and traits of the criminal justice system.

- State and local information systems using a computrized message-switching capability and a computer interface with the FBI's National Crime Information Center hich provides law enforcement officials with on-line infornation on wanted persons, and stolen vehicles, license lates, articles, guns, securities and boats. State data bases lso provide: immediate or real-time access to motor vehicle registrations and driver records and state or local-level NCIC-type files with information not eligible for the NCIC; e.g., missing persons, misdemeanant warrants.
- Large-scale, multi-state organized crime intelligence units to assist law enforcement agencies in ascertaining and establishing the existence of organized crime in a particular jurisdiction, and in determining its strength, organizational structure and sources of income as well as the identification of business and industries vulnerable to penetration.
- State systems related to civil disorders for either tension detection and forecasting or providing support to tactical units, as advised by the Kerner Crime Commission.

In such automation and exchange of information for criminal justice purposes, security and privacy problems should be fully accommodated. There should be strict controls on file content and access should be restricted to bona fide law enforcement agencies.

IT IS ENCOURAGING that the most extensive new data system, Project SEARCH, has also been extremely sensitive to problems of individual privacy . . . . The Project Group developed not only the technical capacity to collect and exchange standardized criminal histories, but also an impressive Code of Ethics and related policies "to assure that the most sophisticated measures are employed and the most perceptive judgments are made in the development and operation of the System to optimize the protection of individual privacy." (Code of Ethics, Art. II, sec. 1)

Among other steps, the Project SEARCH Committee on Security and Privacy prescribes procedures for (quotes from Code of Ethics, amplified in Technical Report No. 2):

- limiting data to that "with the characteristics of public records," recorded "only upon the report of a crime," and excluding such irrelevant data and unreliable material as unverified intelligence tips;
- continuously re-evaluating included data for its accuracy and completeness, and purging such items as "the record of first offenders where criminal proceedings have resulted in the favor of such persons;"
- developing a "high level of computer, legal, physical, information, communications, and personnel security methods" to protect the system and give full protection to all information included; and
- developing "procedures for an individual to learn the contents of the arrest record kept about him and for the correction of inaccuracies or prejudicial omissions in a person's arrest record."

By enacting definite standards for Federal data banks, Congress can inject order into operations now subject to great misunderstanding and suspicion, and promote public confidence in those data collection systems which are necessary. By imposing basic requirements on other systems involving Federal funds or linkages, Congress can guide the states and take a long step toward insuring that state or local data bank abuses remain localized.

While I personally believe that we should begin from recommendations such as those of the SEARCH Project Group, I am frank to admit that right now Congress simply does not know yet enough to prepare sound legislation overnight.

I do not believe that we are doomed to perpetual war between computers and the Constitution. Rather, I am confident that—through hard work and constant watchfulness—we can civilize our technology so as to promote both justice and liberty.

Senator Charles Mathias, Jr. (R.-Md.)
Statement before Senate Subcommittee on Constitutional Rights, March 9, 1971

PRIVACY is one of our most precious human rights, and in today's crowded and disorderly environment, it may be one of the hardest to maintain. Long before the pressures of 1970, Louis Brandeis described privacy as "the right to be let alone, the most comprehensive of rights and the right most valued by civilized man."

The computer does not in itself create any invasion of privacy. Its role is no more active in this respect than the old-fashioned filing cabinet. The threat to privacy posed by surveillance and recordkeeping has been a fact of life for centuries.

The only new element introduced into this picture by the computer is fantastic efficiency. I believe that is what people really fear.

The man on the street, with only a vague comprehension of it as some sort of mechanical brain may regard it as a threat to his job. Or he may see it as an impersonal compounder of errors that show up from time to time on various printed statements—an inhuman device designed to frustrate him by his inability to get past it to the very human person who is really responsible for the mistakes.

If that sort of view represented the only criticism of the computer, there wouldn't be too much for us to worry about. It is easy to demonstrate that computers create far more jobs than they eliminate. And the errors blamed on them are indeed chargeable to people who probably would have made them if the computer had never been invented.

There is criticism, however, of an entirely different sort that *does* worry me. It comes from some very learned and thoughtful people. They don't see the computer as a monster, which it is not. They don't see it as the ultimate master of mankind, which it will never be. They see it, rather, as facilitating a radical realignment of knowledge—and therefore of power. This they regard as a very dangerous possibility—a new sort of computerized power politics because:

We will see systems analysts effecting true management innovation through establishment and manipulation of data by computer.

We will see the data and programs of the last decade's isolated, independent computer systems begin to flow together in enormous national—and even international—data grids. The result: the eventual capability to store and constantly update in computer memory all the information available in the world.

We will see a vast computerized file of case histories at the doctor's disposal to prevent mistakes involving a patient's blood type or allergy to drugs or lack of information on past disabilities, or to assist in making a diagnosis against a given set of symptoms.

We will see a computerized instructional system which supplies each student with material controlled by a program specifically suited to his needs.

There is no way to halt computerization any more than the Luddites of 19th century England could halt the Industrial Revolution.

As Professor Robert Fano of MIT has said, "You can never stop these things. It is like trying to prevent a river from flowing to the sea. What you have to do is to build dams, to build waterworks, to control the flow."

Computer manufacturers are among those who must assume heavy responsibility in controlling the flow, responsibility which needs to be defined and implemented.

We have too many examples around us today of how technology failed to look ahead at problems which it might accelerate, even if it did not really create them. Pollution of our environment is one, and now we must reckon with the human consequences of pollution of privacy.

The computer industry cannot solve the problem alone, but there is much that it can do, technically and ethically.

Technically we can build safeguards into system design. We can make it possible to limit those who are allowed t put information into a system. We can even have the m chines check data against a given set of values and reje questionable information. In fact, all input could be clas fied as it is received, ranging from material of publ record to top secret. Sensitive information then could b encoded during the input process.

Similarly, there can be ingenious safeguards in the deli ery of information. The computer can require a passwor or answers to a series of questions before printing out. could require several persons to be present, each possessin separate parts of a code. According to the password a per son possessed, the computer could limit access to a specifi type of information. It could have intelligence built in t detect any unusual pattern of access request—hesitation for example. It could record each request so as to pinpoin blame later if information is misused. It could be con structed to read badges and other forms of physical identi fication—or even compare the user's voice to a "voice print" stored within it.

There are many more possible examples of technical security systems which I might describe—not to mention increasingly ingenious ones which may be developed in years to come. Yes, our machines can do a lot to protect the privacy of computerized records—particularly if you compare them to a flimsily locked filing cabinet or even a safe. But really determined men, unfortunately, can find ways to get around the best security systems.

So we must consider more than physical safeguards. Obviously the trustworthiness of the operating personnel is an important factor, and management should exercise sensitive control here. What goes into files is also a management decision, and perhaps the question needs to be asked more frequently, "Is this information really necessary?" Do employers, for example, really need to know all about the emotions, personal habits, attitudes and beliefs of other employees—or could they be satisfied to judge their work performance objectively?

The burden of answering questions from all sides is growing for the average man. All of us are leaving a longer and longer trail behind us of information gained by birth records, employment records, Social Security, Selective Service, police, hospitals, credit bureaus, Internal Revenue Service, the Census.

Credit cards establish in the checkless society where we eat and shop and how much we spend. In the cashless society to come, even the smallest transactions may be fed instantly into central computers to put every detail of our daily life on record. If you knock off work mid-afternoon to take in a movie or go out to the golf course, that tiny transgression may be irrefutably noted when your account card is processed at the box office or club house.

If we cannot stop this relentless flow of information about ourselves into central files, we can do as Professor Fano suggests—build a dam here, a filtering system there to control it. For example, trivial information—such as that visit to the movie or the golf course—could be recorded on independent data systems which are periodically erased. A time limit on *all* personal data might be a good idea—so that a youthful indiscretion wouldn't haunt a man's records for the rest of his life.

Frankly I feel that we will need some new legislation in this area. Our old legal framework may not be adequate to defend our privacy against these new techniques.

Perhaps the most important new legal safeguard would provide a citizen with the ability to challenge in court the release of private data about him without his consent. *Without his consent.* These are very meaningful words.

Professo · Alan Westin, in his widely read book *Privacy and Freedom*, had defined privacy as "the claim of individuals, groups or institutions to determine for themselves

Computer v. Personal Dignity

by Richard I. Miller, Esq., Boston, Massachusetts

ON FEBRUARY 8, 1965 Dale B. Menard was picked up without probable cause and held for two days by the Los Angeles police. He was photographed, fingerprinted, interrogated about a burglary and subsequently released with the following entry under the category "Disposition or Sentence: Released—unable to connect with any felony or misdemeanor—in accordance with 849b(1)—not deemed an arrest but detention only."

The data was recorded in an electronic data processing system for analysis and retrieval of criminal histories (today known by the acronym "Project Search") and transmitted to the Federal Bureau of Investigation.

Menard filed suit in the District of Columbia to compel the Attorney General and the Director of the FBI to purge his record from the files. Both sides moved for summary judgment; the U.S. District Court for the District of Columbia granted the government's motion and the plaintiff appealed.

In reversing the ruling of the District Court and remanding the case for trial, Chief Judge David Bazelon observed:

"Information denominated in a record of arrest, if it becomes known, may subject an individual to serious difficulties. Even if no direct economic loss is involved the injury to an individual's reputation may be substantial. Economic losses themselves may be both direct and serious. Opportunities for schooling, employment, or professional licenses may be restricted or nonexistent as a consequence of the mere fact of an arrest, even if followed by acquittal or complete exoneration of the charges involved.

"An arrest record may be used by the police in determining whether subsequently to arrest the individual concerned, or whether to exercise their discretion to bring forward charges against an individual already arrested.

"Arrest records have been used in deciding whether to allow a defendant to present his story without impeachment by prior convictions, and as a basis for denying release prior to trial or appeal; or they may be considered by a judge in determining the sentence to be given a convicted offender . . .

"The present record gives no indication of the extent to which appellant's record may be disseminated, within or without the government, or of the uses to which it may be put." (*Menard v. J. N. Mitchell and J. E. Hoover*, decided June 19, 1970, 430 F 2d. 486 (1970).)

If the plaintiff's arrest was among those included in the Project Search minimum data base of 300,000 records then he may expect that the data will be available by July 1971 to law enforcement agencies of Arizona, Connecticut, Colorado, Florida, Illinois, Maryland, Michigan, Minnesota, New Jersey, New York, Ohio, Pennsylvania, Texas and Washington—in addition to the arresting state and the Department of Justice.

He will also have the comfort of knowing that at least a portion of the funds allocated to this project by the Law Enforcement Assistance Administration have been designated to a standing committee concerned with security and privacy. He may enjoy, too, the intellectual satisfaction of learning that his may well be the first lawsuit of record that raises the peculiar problem of the computer as distinct from the problem of surveillance with which it is so closely associated.

Senator Sam Ervin's Constitutional Rights Subcommittee, which has been holding hearings on domestic intelligence activities, has also expressed its concern with record-keeping as well as snooping. Indeed, it appears that legislative relief from federal maintenance of intelligence files (aside from military surveillance) may be on the way.

Bills have already been introduced by Rep. Edward I. Koch (D.-N.Y.) and Sen. Birch Bayh (D.-Ind.) that would require every government agency to notify the citizen that a record on him is being kept, permit him to correct errors or to refute abusive statements, and to forbid transmission of any information without permission.

While the fate of these particular bills is problematical it is gratifying, at least, that the Congress has started to chip at the tenth of the iceberg above the surface. If the state legislatures and the courts will now begin to provide relief from the further assaults on privacy by the data banks of credit corporations, insurance companies and lending institutions, to say nothing of state and local law enforcement agencies, the excesses of EDP may be curbed.

The basic American premise is: Anything which can be done should be done (particularly if it extends the technological state of the art).

And so we do it . . . and subsequently call upon the law to save us from our enthusiasm. Often, as the balm of the law is applied to the latest technological hangover the lawyer must stretch his doctrinal base.

Such is the case with the novel intrusion that a public memory, i.e. a computer data base, makes on privacy. Privacy, in our jurisprudence, has been defined as the right to be let alone, to decide for oneself how much will be shared with others.

However, the legal concepts normally associated with the individual's claim to a private personality have been almost exclusively concerned with criminal or tortious acquisition of information and civil remedies for the disclosure of information improperly acquired.

The computer, though, is not necessarily concerned with peeping, snooping and prying. It is merely a memory whose data banks, more often than not, are filled with information which is legally, properly and voluntarily disclosed. It is also likely to be inaccurate, incomplete, and indiscriminate. The problem, therefore, is in effect to define a cause of action for "forgetfulness."

"The Common Law," said Justice Brandeis, "secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments and emotions shall be communicated to others." (Warren, Samuel D. and Brandeis, Louis D., "The Right of Privacy," 4 *Harv. L. Rev.* 193, 198 (1890).

Nevertheless, in tort as in criminal law the remedies that the law allows are somewhat short of the mark. Non-statutory protection of privacy cases, so-designated, infrequently arise, and then only as anemic aspects of tort and constitutional law.

The tort cases involve (1) pure intrusion on physical solitude, (2) publication of private matters acquired by intrustion into one's home or belongings, (3) creation of a false public image by untrue or defamatory publication, and (4) appropriation of some element of personality for commercial use without permission. (See Seavey et al. Law of Torts 942-966 (2d Ed. 1964).)

The constitutional cases have, for the most part, arisen under the Fourth Amendment.

In the interest of police surveillance of organized crime the Supreme Court, in the classic wiretapping case, *Olmstead v. United States*, 277 U.S. 438 (1928), materially

Mr. Miller is a principal of the Boston-based consultants firm, Harbridge House, Inc. and a member of the New York and Massachusetts Bars.

This week *SR* conducts a three-pronged investigation of a problem that affects Americans on all levels. Former Attorney General Ramsey Clark reviews Arthur R. Miller's new book, *The Assault on Privacy,* which deals with technological data-gathering and its impact on the private citizen (p. 29); editor-at-large Peter Schrag comments on the "chilling effect" of excessive governmental surveillance in "Dossier Dictatorship" (p. 24); and Ralph Nader, America's foremost consumer advocate, looks into what happens and what the individual can do when . . .

The Dossier Invades the Home

by RALPH NADER

Invasion of privacy used to carry an almost luxurious connotation, a concept reserved for special public figures whose private lives were invaded by scandalmongers or seekers of vicarious thrills. It is no longer an elitist term. Hundreds of bits of information filed in dossiers on millions of individual Americans today constitute a massive assault on privacy whose ramifications are just beginning to be realized.

Most adults have at some time sought credit (or a credit card) and bought insurance. If you have done these things, there are probably at least two dossiers with your name on them.

When you seek to borrow money, your creditor receives a file from the credit bureau to establish your "credit rating." This dossier contains all the personal facts the credit bureau can assemble—your job, salary, length of time on the present job, marital status, a list of present and past debts and their payment history, any criminal record, any lawsuits of any kind, and any real estate you may own. The dossier may include your employer's opinion of your job performance or even your IQ rating from a high school test. By the time the creditor has finished talking to the credit bureau, he is likely to know more about your personal life than your mother-in-law does.

When you try to buy life insurance, a file of even more intimate information about you is compiled by the "inspection agency." The insurance company finds out not only about your health but also about your drinking habits (how often, how much, with others or alone, and even what beverage), your net worth, salary, debts, domestic troubles, reputation, associates, manner of living, and standing in the community. The investigator is also asked to inquire of your neighbors and associates whether there is "any criticism of character or morals," and he must state whether he recommends that the insurance be declined.

Credit bureaus and inspection agencies are the major sources of information about individuals. But government, schools, employers, and banks are also collectors, and sometimes suppliers, of information. Employers frequently make information on their employees available to a credit bureau or inspection agency. They may also exchange information among themselves. *The Wall Street Journal* has reported that department stores in many cities have formed "mutual protection associations" that trade the names of former workers who were fired for suspected theft. This information-trading means that an individual may be denied a job on the basis of a former employer's untested—and unrefuted—suspicions.

Anyone possessing an individual's bank records—now extensively recorded on computers—can reconstruct his associations, movements, habits, and life-style. The recently enacted Foreign Bank Secrecy Act can be used to require every FDIC-insured bank to make a reproduction of each check you draw on it and keep those reproductions for up to six years. The purpose is to ensure records of large quantities of money going out of the country so as to prevent tax evasions through use of secret Swiss bank accounts. But the act contains no protection for the depositor by limiting in any way the banks' use of these records. Conceivably, a bank could sell them to a credit bureau or investigation agency.

It is the rare American who does not live in the shadow of his dossier. The "dossier industry" is a huge and growing business. There are 105 million files kept by the Association of Credit Bureaus of America (ACBA). Retail Credit Company of Atlanta, Georgia, the giant of the industry, has forty-five million files and makes thirty-five million reports each year. Credit Data Corporation, the second largest firm, has twenty-seven million files and adds seven million new dossiers each year.

These economic interests have almost total control over the information they collect and sell. They are not accountable to anyone except those

Demeaning Human Dignity

by RAMSEY CLARK

THE ASSAULT ON PRIVACY: Computers, Data Banks, and Dossiers

by Arthur R. Miller

University of Michigan Press, 333 pp., $7.95

The computer as the future repository of knowledge, calculation, and control is central to any consideration of the quality of life in any society. The very nature of knowledge will be determined in large measure by cybernetics—the comparative study of automatic control systems by which we organize, store, and recall data. Arthur R. Miller, a brilliant young professor at the University of Michigan Law School, scrutinizes in this book the impact of the computer on one vital aspect of our lives—privacy. He came to the subject through chance. In the fall of 1966 a university colleague telephoned him to inquire about the legal consequences of placing copyrighted materials into computers. Mr. Miller quickly saw that law had not come to grips with the implications of this new technology. Moreover, he soon realized that the copyright problem, fascinating as it is, barely touches the range of legal issues arising from the computerization of data. This brought him to the potential threat of computers to privacy. The result is a well-organized, tightly reasoned, and thoroughly documented exploration of the inroads already made by computers on privacy—a pioneer work in a field that has vital implications for the very character of our people.

> Of late [he writes] lawyers and social scientists have been reaching the conclusion that the basic attribute of an effective right of privacy is the individual's ability to control the circulation of information relating to him—a power that often is essential to maintaining social relationships and personal freedom. Correlatively, when an individual is deprived of control over the spigot that governs the flow of information pertaining to him, in some measure he becomes subservient to those people and institutions that are able to manipulate it.

Although his deep concern is apparent, Professor Miller is balanced and unemotional in his analysis; he knows that computers are necessary and can be beneficial, but he is aware of the dehumanization that their irresponsible use can cause.

> . . . Many people have voiced concern that the computer, with its insatiable appetite for information, its image of infallibility, and its inability to forget anything that has been stored in it, may become the heart of a surveillance system that will turn society into a transparent world in which our homes, our finances, and our associations will be bared to a wide range of casual observers, including the morbidly curious and the maliciously or commercially intrusive. These fears have been exacerbated by the clarion call in certain quarters for the establishment of a National Data Center, by the emergence of surveillance data systems as well as computer-based credit-reporting services, and by the hypnotic attraction for electronic record-keeping being exhibited throughout government, industry, and academe.

Endless quantities of personal data are compiled but the individual is un-

RAMSEY CLARK, former Attorney General of the United States, is the author of *Crime in America*. Now in private practice, he is part of the legal team that will defend Philip Berrigan and other alleged conspirators against charges that they plotted to kidnap Henry Kissinger.

SR: BOOKS

Book Review Editor: ROCHELLE GIRSON

Saturday Review

Editor - Norman Cousins

Publisher - William D. Patterson

Associate Editors
Irving Kolodin • Horace Sutton

Associate Publisher - Richard L. Tobin

Managing Editor
Roland Gelatt

Science Editor
John Lear

Education Editor
James Cass

Book Review Editor
Rochelle Girson

Poetry Editor
John Ciardi

Travel Editor
David Butwin

Art Editor
Katharine Kuh

Copy Editor
Peter Nichols

General Editor
Hallowell Bowser

Layout & Production
Pearl S. Sullivan

Editors-at-Large
Cleveland Amory • Alfred Balk
Henry Brandon • Harrison Brown
Charles Frankel • Frank G. Jennings
Elmo Roper • Peter Schrag
Paul Woodring

Contributing Editors
Goodman Ace • Hollis Alpert • Jerome Beatty, Jr.
Henry Hewes • Arthur Knight
Martin Levin • Roliene W. Saal
Robert Lewis Shayon • Zena Sutherland
Walter Terry • Margaret R. Weiss

Dossier Dictatorship

EDITOR'S NOTE: *This week* SR *focuses on the invasion of privacy. The lead article by Ralph Nader (page 18) discusses the use of the dossier by credit bureaus and other private organizations, while former Attorney General Ramsey Clark, in his review of Arthur R. Miller's* The Assault on Privacy *(page 29), assesses the impact of a rampant computer technology devoted to the gathering of information on private citizens. In the following editorial, editor-at-large Peter Schrag deals with the growing use of surveillance by governmental agencies.*

It does not take a long memory to recall the days when that segment of the Orwellian universe that dealt with government surveillance of private citizens and the collection of "dossiers" was largely the concern of fiction writers, students of Stalinist Russia and Nazi Germany, and a small number of others who were generally regarded as paranoids. There had been reports as early as 1966 or 1967 that the police had infiltrated the peace and civil rights movements, that the FBI was tapping Martin Luther King's telephone (among others), and that anti-war demonstrators were being carefully photographed by intelligence agents, but most of those reports were dismissed as exaggerations. If they cared at all, most Americans were certain that their government had neither the resources nor the guile to go into the snooping business in any large way.

We now know that we were wrong, that during the last generation (and most precipitously in the past three or four years) agencies of the government have created an extensive apparatus for the collection, storage, and exchange of what we once regarded as privileged information about the most intimate details of our private lives. The revelations of former intelligence agents (military and civilian) and the extended hearings last month of the Senate Subcommittee on Constitutional Rights have made it entirely clear that the paranoia of 1960 has become the fact of 1971. The Justice Department (particularly the FBI), the Internal Revenue Service, the Passport Division of the State Department, the Social Security Administration, the military, state, and local police, the welfare agencies, the motor vehicles bureaus, and other bureaucracies maintain dossiers on millions of Americans.

The information in those dossiers—many of them now computerized—is often required to carry on the legitimate and necessary functions of the agency that maintains them; but a substantial and growing part, as we learned from the hearings, is also accessible to other people and organizations, public and private, for purposes—to put it mildly—far beyond propriety or Constitutional limits. Sometimes the information leaks; sometimes it is exchanged between agencies; sometimes it is used deliberately to intimidate innocent people. Since it is now technologically possible for the government to link all its data banks through computer terminals and compatible storage systems, the potential already exists for obtaining a master print-out in seconds of all the information—fact, rumor, innuendo—that has been compiled on a particular individual by a number of different agencies. So far, that capability has not been implemented; if it ever is, the government or any unscrupulous official will be able to intimidate or blackmail political enemies at will and to engage in the sort of totalitarian machinations that were once the fantasies of political science fiction.

Yet, even without a central data bank, information has been blatantly misused. Sometimes it is sold—legally or illegally—to private buyers; in some states, any salesman can buy lists of car registrants (with the type, model, and age of the car) from the motor vehicles bureau; elsewhere individual policemen have sold confidential police information to corporate employers interested in the background of prospects for executive positions; sometimes information is surreptitiously released by the police or the FBI to the press to embarrass an individual or organization. We know from the subcommittee hearings that material collected by government investigators about Mayor Joseph Alioto of San Francisco was leaked to writers of a magazine exposé; we also know that last fall military intelligence agents were engaged in the surveillance of political candidates in the state of Illinois, among them Adlai E. Stevenson III, now the state's junior Senator. At this moment there is little other than self-restraint to prevent such information from being furnished to politicians who are sympathetic to government snoops or who happen to enjoy the favor of those who employ the agents. More subtle, but equally frightening, is the general potential for intimidating any citizen engaged in unpopular causes or in whatever political activities happen to displease the government at the moment. The effect is contagious and crippling; most men who think they are being watched are likely to be more cautious in their political opinions no matter how innocent their record and behavior. They have no assurance, moreover, that their dossiers are not loaded with implications and inaccuracies; there is no way that they can see, correct, or answer the material.

On several occasions during the hearings, Senator Sam J. Ervin, Jr., the subcommittee chairman, spoke of the "chilling effect" of government surveillance; what he could not know for certain at the time was that such surveillance has been used deliberately by agents of the government to intimidate dissenters. A few days after the hearings closed, several members of

THE DEATH OF PRIVACY

By RAMSEY CLARK

If we lose the right to be alone and to be let alone, we will lose everything—our individuality, our dignity, our liberty, and our capacity for loving

Who are you? Why are you different from others? How different will you be if you are never alone? If you never reflect? If your every action is witnessed by others? If your thoughts can be known? If you cannot be alone, how will you know what you think? Without privacy, CAN we know what we think? Or even what we are?

Ecclesiastes was wrong. There are new things under the sun. Change is the fundamental fact of our times. The last generation has seen more change in the way people live than has been seen in all of history. In times past, privacy has seemed both plentiful and indestructible, and its value has been largely ignored. Now we are losing it, and once lost, it may never be regained. Crush privacy for a generation and it may be gone forever.

Two powerful dynamics are causing these rapid and dramatic changes; each in its way drastically affects privacy, individuality, and human dignity itself.

The first dynamic is population increase—billions of people, growing numbers beyond the ability of man to contemplate, too many for even the most careful census takers to count accurately.

In today's mass society, how does the individual, anonymous and powerless, find the place to think, to reflect, to discover himself, and to be himself?

The other major dynamic is science and technology. Directing its energies to agriculture, science liberated man from the soil. Roots that gave identity and distances that separated people were lost when the 90 percent that had always labored to feed and clothe us dwindled to 10 percent. People moved from the farms to urban centers, where they lived always in the presence of others.

Automobiles made us the most mobile and its future. It is capable of penetrating the last physical refuges of privacy—the room or the lonely field or beach. It can invade those places without invitation, leaving the individual no place to hide, to be himself.

Science will someday read the mind, detect from afar the various chemical and electric stimulations of the body that are both human emotion and reason, and interpret their meaning: You are going to lift your hand....Though you smile, you do not like what you have just heard....You do not know it, but you are about to have a heart attack, unless....

In one generation, technology liberated man from most of the burdens of nature. Already we wonder whether man will be mastered in turn by technology.

The interdependence and anonymity of man in modern mass society, far from offering privacy, burdens it even further. What can I, as a mere individual among millions, do about the schools my children attend that prepare them for nothing; about the college courses that are repetitious drills in the irrelevant; or the distant and horrible war I neither understand nor want, that takes the life of my beloved? I am powerless to affect the bulldozers that destroy the last place of beauty and recreation where I live, the welfare that strips me of dignity, or the air, water, noise, environmental, and frustration pollutions that permeate my life. The uncontrollable violence, the commotion and ugliness that invade my most private places are beyond my power to keep out.

Mass protest is an answer found by many. It is the most effective way yet discovered for powerless people to be heard beyond the limits of the small human voice. Speaking together in protest, their voices carry to places of power that could not hear or did not care. Though [illegible] its effectiveness [illegible] flock? What crowd doesn't come finally to ignore and often abuse the integrity of its own constituents?

Liberty, curiosity, and doubt are the essential tools of the seeker of truth. Without freedom to ask, the truth cannot be sought. It is curiosity that spurs the free to seek the truth, while doubt saves the curious from error, because it insists on hard evidence. Is there real freedom to ask any question when every question is asked in a crowd or overheard by unknown persons?

Can curiosity flourish in the midst of masses, where the seeker is under constant surveillance? Where is the incentive to inquire? How chilling is the risk of public condemnation or suppression? How heavy is the hand of censorship when every private word may be public? Will doubts arise, and dare they be expressed when there is no privacy, when they will be known to authority and may be suppressed as heresy? Skepticism is not a common quality of a crowd. The truth may prove hard to find among a people without privacy.

Privacy is essential to the development of individual personality. Judgment and common sense arise from the reflection of the individual. Character is developed [illegible]

If you never reflect? If your every action is witnessed by others? If your thoughts can be known? If you cannot be alone, how will you know what you think? Without privacy, CAN we know what we think? Or even what we are?

Ecclesiastes was wrong. There are new things under the sun. Change is the fundamental fact of our times. The last generation has seen more change in the way people live than has been seen in all of history. In times past, privacy has seemed both plentiful and indestructible, and its value has been largely ignored. Now we are losing it, and once lost, it may never be regained. Crush privacy for a generation and it may be gone forever.

Two powerful dynamics are causing these rapid and dramatic changes; each in its way drastically affects privacy, individuality, and human dignity itself.

The first dynamic is population increase—billions of people, growing numbers beyond the ability of man to contemplate, too many for even the most careful census takers to count accurately.

In today's mass society, how does the individual, anonymous and powerless, find the place to think, to reflect, to discover himself, and to be himself?

The other major dynamic is science and technology. Directing its energies to agriculture, science liberated man from the soil. Roots that gave identity and distances that separated people were lost when the 90 percent that had always labored to feed and clothe us dwindled to 10 percent. People moved from the farms to urban centers, where they lived always in the presence of others.

Automobiles made us the most mobile and its future. It is capable of penetrating the last physical refuges of privacy—the room or the lonely field or beach. It can invade those places without invitation, leaving the individual no place to hide, to be himself.

Science will someday read the mind, detect from afar the various chemical and electric stimulations of the body that are both human emotion and reason, and interpret their meaning: You are going to lift your hand....Though you smile, you do not like what you have just heard....You do not know it, but you are about to have a heart attack, unless....

In one generation, technology liberated man from most of the burdens of nature. Already we wonder whether man will be mastered in turn by technology.

The interdependence and anonymity of man in modern mass society, far from offering privacy, burdens it even further. What can I, as a mere individual among millions, do about the schools my children attend that prepare them for nothing; about the college courses that are repetitious drills in the irrelevant; or the distant and horrible war I neither understand nor want, that takes the life of my beloved? I am powerless to affect the bulldozers that destroy the last place of beauty and recreation where I live, the welfare that strips me of dignity, or the air, water, noise, environmental, and frustration pollutions that permeate my life. The uncontrollable violence, the commotion and ugliness that invade my most private places are beyond my power to keep out.

Mass protest is an answer found by many. It is the most effective way yet discovered for powerless people to be heard beyond the limits of the small human voice. Speaking together in protest, their voices carry to places of power that could not hear or did not care. Though

Liberty, curiosity, and doubt are the essential tools of the seeker of truth. Without freedom to ask, the truth cannot be sought. It is curiosity that spurs the free to seek the truth, while doubt saves the curious from error, because it insists on hard evidence. Is there real freedom to ask any question when every question is asked in a crowd or overheard by unknown persons?

Can curiosity flourish in the midst of masses, where the seeker is under constant surveillance? Where is the incentive to inquire? How chilling is the risk of public condemnation or suppression? How heavy is the hand of censorship when every private word may be public? Will doubts arise, and dare they be expressed when there is no privacy, when they will be known to authority and may be suppressed as heresy? Skepticism is not a common quality of a crowd. The truth may prove hard to find among a people without privacy.

Privacy is essential to the development of individual personality. Judgment and common sense arise from the reflection of the individual. Character is developed through the inward eye of privacy seeking to know itself over years of varied experience. True integrity is grounded in character so developed. The great public liberties—exercise of religion, freedom of speech and the press, the rights of petition, association, and assembly, equal protection, and due process—are but empty vessels without the personal freedom of privacy. Privacy is the ultimate freedom. Only with privacy can we do whatever we will, so long as we do not interfere with others

shone Tribe of the Fallon Reservation and Colony provides the Fallon Business Council with certain powers to negotiate with the Federal Government on behalf of the tribe, and

Whereas, dating back to the late 1920's a band of Indians settled in the Carson Sink area, and

Whereas, in the early 1900's with the creation of the Newlands Reclamation Project, a land exchange program was entered into between the Indians with land holdings in the project area and the United States of America. The program gave rise to the Fallon Reservation where the Indian families were to be located on 10-acre tracts with full water rights from the Newlands Project, and

Whereas, the Paiute-Shoshone Tribe of the Fallon Reservation and Colony are presently holding a water right on 4,877.3 acres, paid in full, and

Whereas, through experience and affirmed by field surveys, additional lands are required to make beneficial use of the above water rights, and

Whereas, it is the Business Council's understanding that a general review of withdrawn land status near the reservation is being made by the Department of Interior at this time, and

Whereas, members of the Paiute-Shoshone Tribe of the Fallon Reservation and Colony have an urgent need and have demonstrated that it will make use of the water and additional lands to better their standard of living, now therefore,

Be It Resolved that the following described lands:

S1/2 of Section 33, T. 20 N., R. 30 E., MDBM,

S1/2 of Section 34, T. 20 N., R. 30 E., MDBM,

W1/2 of SE1/4 & SW1/4 of Sec. 35, T. 20 N., R. 30 E., MDBM,

NW1/4 of Section 2, T. 19 N., R. 30 E., MDBM,

N1/2 and SW1/4 of Sec. 3, T. 19 N., R. 30 E., MDBM,

All of Section 4, T. 19 N., R. 30 E., MDBM and

N1/2 and SW1/4 of Sec. 8, T. 19 N., R. 30 E., MDBM,

totaling some 2,640 acres be added to the Fallon Reservation and Colony to meet the above stated needs.

CERTIFICATION

I, the undersigned, do hereby certify that the Business Council is composed of 5 members, of whom 4, constituting a quorum were present at a meeting called and held this 13 day of Dec., 1970, and that the foregoing resolution was adopted at such meeting by a vote of 4 for and none against, pursuant to Article VI, Section 1(a) of the Constitution and Bylaws of the Paiute Shoshone Tribes of the Fallon Reservation and Colony.

S/ VIVIAN HICKS,
Secretary-Treasurer of the Fallon Business Council.

By Mr. BIBLE (for himself and Mr. CANNON):

S. 2545. A bill to authorize the Attorney General to exchange criminal record

announced that pursuant to an opinion and order of the U.S. District Court for the District of Columbia in the case of Menard against Mitchell (Civil Action No. 39-68), the FBI is now prohibited from disseminating criminal record information in response to fingerprints submitted by State and local law enforcement and other State and local government agencies where the request is made for other than direct law enforcement purposes.

This prohibition has already been in effect since July 22. The processing of all such fingerprints has ceased, and all requests for records in such cases are being returned without action to the State or local agencies.

This means, Mr. President, that notwithstanding specific and well-considered provisions of State and local laws throughout the Nation—provisions requiring a full inquiry into the background of persons seeking licensing or employment in sensitive businesses or occupations affected with a public interest—State and local agencies have been denied access to information available only through the FBI.

It means that where an FBI record check is required under State or local law or regulation our State and local agencies have been placed in the position of not being able to fulfill their obligations under their own laws.

My own State of Nevada has established a comprehensive system of laws and regulations to assure that the State's legalized gaming industry is closely controlled and operated fairly and honestly in the public interest. Our laws require an exhaustive investigation of all who seek gaming licenses and employment in the industry. They provide the FBI, the U.S. Treasury, and the Internal Revenue Service access to confidential records maintained by State agencies. They provide a regulatory system which is vigorously enforced by dedicated public servants.

The operation of Nevada's gaming industry is closely and effectively monitored but as a result of this recent court decision the State is now denied access to vital background information on those who would enter this sensitive industry.

In other areas, Nevada statutes or regulations required criminal record checks on applicants for licensure as lawyers, doctors of medicine, real estate brokers, private investigators, for employment in the business of dispensing alcoholic beverages, and in connection with other professions, businesses, and occupations.

And Nevada is certainly not unique. I daresay most, if not all, of the States and localities throughout the Nation have

discontinuance of these essential FBI identification services is inconsistent with the Crime Control Act of 1970, which had the overwhelming support of the Congress.

The Senate will recall that the purpose of title IX of that legislation is to curb and penalize the infiltration of legitimate business by organized criminals and racketeers.

Regulated industries are among those exposed to such infiltration. Official agencies charged with the duty to monitor and police the operations of sensitive regulated industries now find themselves denied access to essential criminal record information.

It would be inconsistent with our efforts to combat organized crime to permit this information barrier to stand.

Mr. President, I ask unanimous consent that the opinion and decision of the U.S. District Court for the District of Columbia in Menard against Mitchell, Civil Action No. 39-68 and the letter of July 22, 1971 from the Federal Bureau of Investigation to "All Fingerprint Contributors" be printed in the RECORD following my remarks.

I am not going to undertake at this time any detailed analysis of the court's opinion. It will be in the RECORD for Members to read, and will be available for analysis by the appropriate committee.

Suffice it to say that in Menard the court examined the existing statutory and regulatory framework under which the FBI has provided fingerprint identification services to nonlaw enforcement agencies of State and local governments and found it wanting.

The court noted that widespread dissemination of criminal records information may place substantial obstacles in the way of a person's opportunity for employment or advancement and can raise serious questions involving several constitutional guarantees—such as the presumption of innocence, due process, and the right to privacy.

Specifically, the Court found that the existing law is designed only to facilitate coordinated law enforcement activities between the Federal and local governments to assist arresting agencies, court and correctional institutions in the apprehension, conviction, and proper disposition of criminal offenders.

The Court concluded that nothing in the present statute or its legislative history indicates that the Congress intended that FBI criminal record information be made available for nonlaw enforcement purposes, and held that the FBI is without authority to disseminate arrest rec-

would know whether and where to budget for additional parole officers.

Modern information technology now permits a massive assault on these problems on a level never before conceivable. Computers have been used to solve related problems in such diverse fields as continental air defense, production scheduling, airline reservations, and corporate management. Modern computer and communications technology permits many users, each sitting in his own office, to have immediate remote access to large computer-based, central data banks. Each user can add information to a central file to be shared by the others. Access can be restricted so that only specified users can get certain information.

The most delicate part of any criminal justice information system is the record of previously arrested people and accompanying information about them. Such information is valuable in making prosecution, sentencing, and correctional decisions. But whenever government records contain derogatory personal information, they create serious public policy problems:

The record may contain incomplete or incorrect information.

The information may fall into the wrong hands and be used to intimidate or embarrass.

The information may be retained long after it has lost its usefulness and serves only to harass ex-offenders, or its mere existence may diminish an offender's belief in the possibility of redemption.

Heretofore, the inherent inefficiencies of manual files containing millions of names have provided a built-in protection. Accessibility will be greatly enhanced by putting the files in a computer, so that the protection afforded by inefficiency will diminish, and special attention must be directed at protecting privacy. However, the new technology can create both more useful information and greater individual protection.

Since the issuance of the Crime Commission's report in 1967, a great deal of study has been given to the security and privacy aspects of criminal justice information systems. The Law Enforcement Assistance Administration, created by the Omnibus Crime Control and Safe Streets Act of 1968, soon originated as Project SEARCH—System for Electronic Analysis and Retrieval of Criminal Histories—a prototype, computerized system for the exchange of criminal history information among the States. In December 1970, having successfully demonstrated the prototype, Project SEARCH was turned over to the FBI for development of an operational system to be part of the National Crime Information System. One of the crucial decisions required to be made by the SEARCH project group was how to deal with the security and privacy problem. The recommendations of that group, which was composed of distinguished members of the law enforcement and data processing communities, contributed significantly to the development of the legislation I now introduce.

In the course of the consideration in the Senate of the proposed Omnibus Crime Control Act of 1970, an amendment was added to that legislation by the Committee on the Judiciary, to require the Law Enforcement Assistance Administration to submit legislative recommendations to promote the integrity and accuracy of criminal justice data collection. Popularly known as the Mathias amendment, for its author, our colleague from Maryland, the new provision was subsequently amended in conference to make clear that the legislative recommendations should assist in the purposes of the law enforcement assistance program.

The bill which I introduce is Attorney General Mitchell's response to the legislative mandate of the 1970 act.

The significant features are:

Provide for stringent controls over the security of criminal justice data systems, including that they be used only for law enforcement purposes and under the management control of law enforcement agencies. In order to permit State and local agencies which cannot meet these requirements to participate in a system, the Attorney General is authorized to grant waivers in proper cases.

Provides for limited access to covered data systems. Only law enforcement agencies—police, courts, corrections—will have direct access. Further dissemination of information must be necessary to the enforcement of a specific law and approved by the Attorney General.

Authorizes an individual to have access to his record so that he may ensure that it is accurate and complete.

Requires operating procedures to assure that each individual's record is purged from the active files after the passage of a sufficient period of time to indicate that the individual is no longer active in the criminal justice system—that is, deceased or rehabilitated.

Provides for civil and criminal penalties for the willful dissemination or use of criminal justice information in violation of the provisions of the bill.

Authorizes the Attorney General to prescribe regulations to carry out the provisions of the bill.

Mr. President, the issues framed by this bill are deserving of the serious and prompt consideration of the Senate. I urge my colleagues to join with me in according it that consideration.

I ask unanimous consent that the Attorney General's letter transmitting the legislation, the bill, and a section-by-section analysis be printed in the RECORD. I ask that the bill be appropriately referred.

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

S. 2546

A bill to facilitate and regulate the exchange of criminal justice information and to insure the security and privacy of criminal justice information systems

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Criminal Justice Information Systems Security and Privacy Act of 1971."

DEFINITIONS

SEC. 2. For the purposes of this Act—

(1) "criminal justice information system" means a system, including the equipment, facilities, procedures, agreements and organizations thereof, funded in whole or in part by the Law Enforcement Assistance Administration, for the collection, processing or dissemination of criminal offender record information or criminal intelligence information.

(2) "criminal offender record information" means records and related data, contained

By Mr. HRUSKA:

S. 2546. A bill to facilitate and regulate the exchange of criminal justice information and to insure the security and privacy of criminal justice information systems. Referred to the Committee on the Judiciary.

Mr. HRUSKA. Mr. President, I introduce today a bill which confronts Congress with the important issue of how law enforcement agencies—Federal, State, and local—can maintain and disseminate necessary information on criminal offenders and still protect the privacy rights of the individuals concerned.

This has become an increasingly more critical issue in the computer age, as the hearings held early this year by the Subcommittee on Constitutional Rights amply demonstrated. The problem was stated succinctly by the President's Commission on Law Enforcement and Administration of Justice, as follows:

The importance of having complete and timely information about crimes and offenders available at the right place and the right time has been demonstrated throughout this chapter and, indeed, throughout this report. With timely information, a police officer could know that he should hold an arrested shoplifter for having committed armed robbery elsewhere. With a more detailed background on how certain kinds of offenders respond to correctional treatment, a judge could more intelligently sentence a second offender. With better projections of next year's workload, a State budget office

AJIS

ALASKA JUSTICE INFORMATION SYSTEM

PHYSICAL, OPERATIONAL AND DATA SECURITY

1. Physical Security.

1.1 Computer Room.

1.1.1 Problem - Unauthorized access to computer room.

Solution - The Department of Administration has an informal policy to restrict access to the computer room to people necessary for its operation. This policy will be formalized and enforced. Personal recognition is the only identification basis envisioned.

1.1.2 Problem - Unauthorized operators.

Solution - Only persons with successful background investigations will have access to the computer room. Passwords will be required to operate the AJIS terminal located in the computer room (see 2.1) Since the computer room is open to vendor personnel, background investigations may be necessary

SECURITY TABLE

AUGUST 1972 CONTROLS

INFORMATION

AGENCY

	LAW ENFORCEMENT									
	AST	LOCAL POLICE	IDEN-TIFICATION	DR. LIC.	F&G LIC.	COURTS	CORRECTIONS	DEPT. OF LAW	MASTER TERMINAL (AST)	CONTROL TERMINAL
Name/Alias/Moniker	X	X	X	X	X		X	X	X	
Physical Description	X	X	X	X	X		X	X	X	
DOB	X	X	X	X	X		X	X	X	
Special Characteristics	X	X	X				X	X	X	
Address	X	X	X	X	X		X	X	X	
Driver License	X	X		X					X	
F & G License	X				X				X	
Parole/Prob/Inst	X	X	X			X	X	X	X	
Want/Warrants	X	X	X	X	X	X	X	X	X	
SSN	X	X	X				X	X	X	
FBI#	X	X	X				X	X	X	
AST#	X	X	X				X	X	X	
Fingerprints	X	X	X				X	X	X	
Police Agency Nos	X	X	X				X	X	X	
IDMO	X	X	X				X	X	X	
Known Convictions	X	X	X			X			X	
Last Arrest Date	X	X	X			X	X	X	X	
Stolen Vehicle Information	X	X	X						X	
Administrative Correctional Info.							X			
Terminal Security									X	
Operator Security									X	
System Errors										X
Administrative Message	X	X	X	X	X	X	X	X	X	X

Model code

First two pages

are very important —

As Gov.'s proposed bill leaves the criteria up to the Commission under very general guidelines (See marked sections HB563)

TITLE 6. GOVERNOR'S OFFICE

PART 4. COMMISSION ON THE ADMINISTRATION OF JUSTICE

CHAPTER 60. CRIMINAL JUSTICE INFORMATION SYSTEMS

Article
1. Security (§§05-20)
2. Access and Use (§§25-45)
3. Purging of Criminal Offender Record Information (§§50-65)

ARTICLE 1. SECURITY

Section
05. Scope of Regulations
10. Criminal Justice Information
15. Segregation of Computerized Files and their Linkage to Investigatory Files
20. Terminal Security

6 AAC 60.005. SCOPE OF REGULATIONS. The regulations in this chapter apply only to electronic computer retrieval of criminal justice information from a criminal justice information system as defined in AS 12.62.070. (Eff. / /72, Reg. 44)

Authority: AS 12.62.010
AS 12.62.070

6 AAC 60.010. CRIMINAL JUSTICE INFORMATION. The following categories of information, as strictly defined, may be recorded and stored in an electronic, computer retrieval, criminal justice information system as criminal justice information:

(1) an individual's full name, any and all aliases known to refer to that person including, but not limited to nicknames;

(2) a physical description including, but not limited to, height, weight, sex, color of hair, color of eyes, identification of race, and other identifying physical features;

(3) an individual's date of birth and citizenship;

(4) information that is reasonable and which has been reported by a reliable source indicating that an individual may be armed, dangerous, has shown suicidal tendencies, or has given indications of unstable emotional behavior;

(5) last known residence;

(6) an individual's current driver's license class and number, the issuing authority, the date of expiration, and any suspension, revocation or cancellation of the license;

(7) last recorded fish and/or game license numbers, in-

DRAFT
Law

IN THE LEGISLATURE OF THE STATE OF ALASKA

EIGHTH LEGISLATURE - FIRST SESSION

For an Act entitled: "An Act relating to the inspection of public records."

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF ALASKA:

* Section 1. AS 40 is amended by adding a new chapter to read:

Chapter 25. INSPECTION OF PUBLIC RECORDS

Sec. 40.25.010. PURPOSE. The purpose of this chapter is to provide for public access to information concerning the conduct of governmental affairs and to provide for the right of individuals to privacy by restricting access to public records containing information of a private or personal nature.

Sec. 40.25.020. INSPECTION AND COPIES OF PUBLIC RECORDS. Unless specifically provided otherwise the books, records, papers, files, accounts, writings, and transactions of all agencies are public records and are open to inspection by the public under reasonable rules during regular office hours. The public officer having the custody of public records shall give on request and payment of costs a certified copy of the public record.

Sec. 40.25.030. EXCEPTIONS, INSPECTION AND COPYING OF PUBLIC RECORDS. Every person has a right to inspect a public writing or record in the state, except (1) records of vital statistics and

AS 18.50 and AS 20.10; (2) records pertaining to a juvenile; (3) medi-

GOVERNOR'S COMMISSION ON THE
ADMINISTRATION OF JUSTICE
MEETING

February 24, 1972

Senator John Rader