

95th Congress }
2d Session }

COMMITTEE PRINT

THE EROSION OF LAW ENFORCEMENT
INTELLIGENCE AND ITS IMPACT ON THE
PUBLIC SECURITY

REPORT

OF THE

SUBCOMMITTEE ON
CRIMINAL LAWS AND PROCEDURES

TO THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
NINETY-FIFTH CONGRESS

SECOND SESSION

59996



NCJRS

JUL 23 1979

ACQUISITIONS

U.S. GOVERNMENT PRINTING OFFICE

34-635 O

WASHINGTON : 1978

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402

Stock No. 052-070-04771-2

COMMITTEE ON THE JUDICIARY

JAMES O. EASTLAND, Mississippi, *Chairman*

EDWARD M. KENNEDY, Massachusetts

BIRCH BAYH, Indiana

ROBERT C. BYRD, West Virginia

JAMES ABOUREZK, South Dakota

JOSEPH R. BIDEN, Jr., Delaware

JOHN C. CULVER, Iowa

HOWARD M. METZENBAUM, Ohio

DENNIS DECONCINI, Arizona

PAUL G. HATFIELD, Montana

MARYON ALLEN, Alabama

STROM THURMOND, South Carolina

CHARLES McC. MATHIAS, Jr., Maryland

WILLIAM L. SCOTT, Virginia

PAUL LAXALT, Nevada

ORRIN G. HATCH, Utah

MALCOLM WALLOP, Wyoming

SUBCOMMITTEE ON CRIMINAL LAWS AND PROCEDURES

JAMES O. EASTLAND, *Acting Chairman*

JAMES O. EASTLAND, Mississippi

EDWARD M. KENNEDY, Massachusetts

STROM THURMOND, South Carolina

ORRIN G. HATCH, Utah

(II)

CONTENTS

	Page
Introduction by Senator James O. Eastland.....	1
List of hearings and witnesses covered in the following report.....	9
I. Law enforcement intelligence: Its nature and its purpose.....	13
The importance of intelligence as viewed by national organizations.....	20
II. Factors contributing to the erosion of law enforcement intelligence.....	26
The role of the media.....	28
Organized legal harassment.....	29
Chicago: A case history.....	33
III. The extent of the erosion.....	37
IV. The consequences of the erosion: A general summary.....	40
V. Is law enforcement intelligence legal? A summary of court rulings.....	43
VI. Factors contributing to the erosion (II): The Freedom of Information Act and the Privacy Act.....	49
The Freedom of Information Act.....	49
The Privacy Act.....	51
The practical consequences of FOIA/Privacy Act.....	52
Who are the requestors?.....	56
The criminal exploitation of FOIA.....	63
FOIA: Other advantages to the criminal world.....	66
Recommendations for amendments to the Freedom of Information Act and the Privacy Act.....	70
VII. Factors contributing to the erosion (III): Impact of the Tax Reform Act of 1976.....	73
VIII. Consequences of the erosion (I): The crippling of abilities to deal with terrorism and civil disturbances.....	75
Terrorism.....	75
Civil disturbances.....	84
IX. Consequences of the erosion (II): The weakening of the war against drugs.....	88
X. Consequences of the erosion (III): The impact on corporate and public security.....	92
The "ban" on background checks.....	98
The "climate of fear".....	103
The problem of nonprosecution.....	104
The "rip-off" society.....	105
Specific problems of security in various industries.....	106
The need for balance: A few recommendations.....	120
XI. Consequences of the erosion (IV): The dismantling of the Federal employee security program.....	124
Recommendations.....	135
Appendix:	
Data on Privacy Act and Freedom of Information Act provided by Federal law enforcement agencies.....	140
Report by the Comptroller General of the United States: Impact of the Freedom of Information and Privacy Acts on law enforcement agencies.....	141

(iii)

NGJRS

JUL 23 1979

ACQUISITIONS

INTRODUCTION

(By Senator James O. Eastland)

The information contained in this report is the product of investigative and oversight hearings bearing on "The Erosion of Law Enforcement Intelligence and its Impact on the Public Security." The investigation and hearings were conducted initially under the auspices of the Senate Internal Security Subcommittee and subsequent to July of 1977, by the Subcommittee on Criminal Laws and Procedures. As Acting Chairman, of the subcommittee, I want to acknowledge and express my appreciation for the major contribution made by Senator Strom Thurmond in carrying forward this important study by presiding over the bulk of the subcommittee's hearings. In the course of these hearings the subcommittee heard scores of witnesses from the field of law enforcement, from Government agencies, and from private industry.

The findings disclosed through these hearings are shocking. Although each of the hearings in the series developed information that the subcommittee found disturbing, it is infinitely more disturbing when the totality of the evidence presented is viewed in an organized and systematic manner, which this report seeks to do. Our Federal and State governments in recent years have permitted, or even encouraged, a massive erosion of law enforcement intelligence and of security in consequence of which we are rapidly moving toward the status of a "zero security" society.

How has this situation come about? It has come about in a piecemeal manner, increment by increment—which has enabled the process to escape the scrutiny of Congress and the press. The testimony of the many witnesses more or less concurred on the principal factors responsible for the erosion of law enforcement intelligence. Among the factors identified were:

- (1) The admitted existence of some genuine abuses in the field of law enforcement intelligence, the lack of guidelines and the lack of adequate oversight.

- (2) The widespread anti-intelligence hysteria in the wake of Watergate.

- (3) The tendency of the media to take up the cudgel against law enforcement intelligence.

- (4) The Fair Credit Reporting Act, the Freedom of Information Act, the Privacy Act, and other privacy legislation—or to be more precise certain provisions of these acts and excessive interpretations of these provisions.

- (5) Parallel legislation at the State level, sometimes more restrictive than the Federal model.

(6) Law Enforcement Assistance Administration (LEAA) pressures designed to bring local and State procedures governing the gathering and dissemination of intelligence into conformance with its interpretation of the Federal requirements.

(7) A general predisposition on the part of the courts, especially the lower courts, to decide privacy litigation in favor of the claimant's right to privacy.

(8) A pervasive climate of fear based on uncertainty about the precise requirements of the Federal and State laws, which has inhibited law enforcement agencies at the Federal, State and local levels, both in the compilation of intelligence and the sharing of intelligence with other agencies.

(9) Recent restrictions, at every level, on the use of surveillance and third party records.

(10) Actions directed against law enforcement intelligence activities by organizations such as the American Civil Liberties Union, the National Lawyers Guild, and the Alliance to End Repression. These activities have included among other things, the bringing of suits against law enforcement agencies, of which the best known, perhaps, is the Socialist Workers Party's suit against the FBI, claiming more than \$30 million in damages.

No law enforcement agency and no national government can function without the instrument of intelligence. As one witness put the matter, intelligence serves as the eyes and ears of the law enforcement community—without intelligence, law enforcement is like a blind man groping after determined and elusive enemies.

Acting out of the best of intentions, we may in recent years have dangerously weakened Government's ability to protect the individual, the community and the Nation.

As one of the witnesses summed up the situation: "Who benefits from this situation? Certainly not the American people. The only real beneficiaries are the criminal and terrorist and other conspiratorial elements in our society."

Let me here summarize some of the highlights of the testimony presented in the course of the many hearings.

The past decade has witnessed a massive destruction of intelligence files dealing with extremist organizations of both the far Left and the far Right. The State of Texas Public Safety Division destroyed its files four years ago; the New York State Police files have been locked up for over three years; Washington, D.C., Baltimore, Pittsburgh and other cities have also destroyed their files; the files of the Chicago Police Department have been locked up since March of 1975; while in New York City, Los Angeles, and other major cities there has been a wholesale destruction of files, ranging from 90-98 percent of the previous total.

Many law enforcement agencies at State and local level have completely abandoned the intelligence function and terminated their domestic intelligence units.

The gathering of new intelligence, where intelligence units still exist, has been further hobbled by the now nearly universal criterion that no intelligence entry is permissible about an individual known or believed to be a member of an extremist organization in the absence of an indictment or a conviction.

Law enforcement intelligence traditionally has operated through four primary instrumentalities: (1) informants, (2) citizen cooperation, (3) surveillance, including electronic surveillance, (4) "third party records", including bank records, telephone and utility records, and credit records.

Today, informants are rapidly becoming an extinct species because of the fear that their identity will be revealed in response to a Freedom of Information request; citizens cooperation has also been effectively "chilled" by the fear of disclosure; surveillance is drastically restricted—in twenty-one States, indeed, electronic surveillance is completely prohibited even in cases of kidnaping or drug trafficking; and existing privacy legislation at both the Federal and State levels has made access to third party records increasingly difficult, especially when the need is for quick information in order to apprehend a criminal or prevent a crime.

The situation has been further complicated by the general fall-off in the sharing of intelligence between Federal, State, and local agencies.

Not many years ago such a sharing of intelligence was more or less taken for granted. Today, primarily because of the impact of the Freedom of Information Act and the Privacy Act, the sharing of intelligence operates at a sadly reduced level. As Captain Justin Dintino, Chief of Intelligence for the New Jersey Police, told the subcommittee:

The free flow of intelligence between, Federal, State, and local agencies is essential to an effective law enforcement operation. To the extent that this flow is restricted, law enforcement is handicapped. And today this flow is terribly restricted, at every level and in every direction: From city-to-city, from State-to-State, from State agencies to Federal agencies, and from Federal agencies to the State and local level. This is a disastrous situation and we're got to find some way of reversing it.

A prime function of all law enforcement, clearly, is the protection of the Nation, the community and the individual citizen. The phenomenon of national and international terrorism is growing. But the destruction of files on extremist organizations, the almost total freeze on the sharing of intelligence, and the wiping out of intelligence units, has deprived the law enforcement community of the ability to effectively discharge this protective responsibility.

A warning example of what can happen when law enforcement does not have this ability was the Hanafi Muslim siege in the Nation's capital. Only several years before the incident took place, the Washington Metropolitan Police Department had had an informant in the Hanafi Muslims, as well as an extensive file on their membership and activities. But then, under instructions from the Washington, D.C., City Council, the Metropolitan Police Force had been compelled to wipe out its Intelligence Unit, destroy its files and cut off all of its informants in extremist organizations. Stripped of intelligence capabilities, there was absolutely no way in which the Washington police could have foreseen the incident or could have acted to prevent it. One person died, one was paralyzed for life, and several hundred others suffered a personal ordeal that left them with heavy psychological scars.

The testimony of Mr. H. Stuart Knight, Director of the Secret Service, established that the widespread erosion of law enforcement intelligence has seriously affected the ability of the Secret Service to provide effective protection for the President and other national leaders and visiting foreign dignitaries for whom it has responsibility. Mr. Knight told the subcommittee that the Secret Service is today receiving only 40-50 percent the amount of intelligence it used to receive for the purpose of discharging its protective functions. Beyond this, he stated that the falloff in the quality, or completeness, of the information they were getting might account for a further degradation of 25 percent. What this boils down to is that the Secret Service—despite the fact that it rates a very high degree of cooperation from all law enforcement agencies—is today receiving approximately 25 percent of the intelligence input it used to receive.

Mr. Knight said that sometimes, because of the lack of intelligence, the Secret Service had to rely on what he called "institutional memory"—a procedure which he did not recommend. He also said that in many situations the Service attempted to compensate for lack of intelligence by pumping in more manpower—a procedure which he was unhappy about for obvious reasons. Finally, when he was asked whether the Secret Service had recommended, or would recommend, that the President not visit certain cities because of a critical lack of intelligence, he replied that there were such cities but he preferred not to name them in public session.

This is somehow symbolic of the perilous state to which we have been reduced by the erosion of law enforcement intelligence.

Mr. Knight's statement that the Secret Service, in the absence of local intelligence records, has had to rely on "institutional memory" is disturbing not only because this is a highly questionable way to go about protecting the President of the United States. Equally disturbing—perhaps even more disturbing from the standpoint of its overall implications for our society—are the possibilities that are opened up when law enforcement authorities, having been compelled to destroy their files, or having been prohibited from making entries into their intelligence files, have to rely on recollections of details that may in some cases go back several years or more.

The "hip pocket" type of intelligence operation is the worst of all possible ways to collect or use intelligence information. Even where the most conscientious officers are involved, the reliance on memories which are sometimes years old is bound to result in a high quota of inaccuracies. With carefully drawn guidelines and with provisions for oversight, there will still be errors—but there exists a mechanism for correcting or eliminating erroneous intelligence. However, there is no possible way of correcting the inaccuracies that are inevitably disseminated in consequence of the "hip-pocket" procedures that have now been forced on our law enforcement intelligence community. The report on the "Impact of the Freedom of Information and Privacy Acts" prepared by the General Accounting Office at my request makes the point that "because of their concerns, most local officials said they are increasingly providing information orally and only to Federal agents with whom they have established rapport."

It is an appalling thought that law enforcement officers, in seeking to enforce the law and protect society, should be compelled to exchange intelligence on a "hip-pocket", or underground, basis in order to protect themselves and their agencies against the possibility of civil suits.

The public protection demands that corporate employees in certain categories of employment be the subjects of criminal record checks. No one would want a convicted rapist or burglar entering his house in the guise of a telephone installation man or utility repairman. Similarly, no hospital patient would be happy in the knowledge that one of the attendants waiting on him had a record of convictions for drug addiction or felonious assault. Nor could anyone—no matter what his political outlook—be indifferent to the possibility that the inability to conduct effective background checks might have enabled several members of a militant terrorist group to infiltrate the staff of a nearby nuclear installation.

These are not hypothetical possibilities. Background checks are not forbidden by law. However, as the testimony before the subcommittee established, the combined effect of the Fair Credit Reporting Act, the Privacy Act, and other privacy legislation has been to create a situation which makes it virtually impossible to conduct meaningful background checks.

Inevitably, the public has suffered cruelly as a result of this exaggerated emphasis on privacy. A document submitted by one of the witnesses told the story of a fire which had killed 16 people in a Chicago nursing home early last year. Suspecting arson, the police questioned the employees. It turned out that a woman employee had previously been employed by several institutions where suspicious fires had occurred and she had been questioned in connection with them. Before the investigation was over, the woman had been indicted on 16 counts of homicide. Privacy legislation has had the effect of protecting the woman employee in question against the possibility of being denied employment. But the question must be posed: Did society have the right to interpret the right of privacy in such an absolute manner that it made possible the killing of 16 innocent victims?

Mr. Robert Ross, a witness who testified from a background of many years of experience in hospital security, told the subcommittee about many similar instances, where hospitals, deprived of the ability to do background checks, had employed people with criminal records—with the result that patients and nurses had been raped or attacked or murdered or robbed. The fact of the criminal record became known only at the point where the culprit was apprehended—too late to do any good for his victim. Mr. Ross terminated his testimony with the warning words that, if the present situation remained unchanged, "the next victim of a hospital crime may be you."

The testimony also established that the public is today paying a much higher price for insurance and banking and higher costs for many other services and goods because corporations cannot conduct background checks to prevent infiltration by organized crime or embezzlers or by the new breed of computer criminals.

The erosion of law enforcement intelligence, the excessive interpretation of the right of privacy which has now apparently become the norm, and the general climate that has developed in consequence, have combined to create a situation in which—for all practical purposes—the Federal Employee Security Program has been completely nullified. Today, apparently, no one can be barred from employment by the United States Government, even in sensitive positions, on the basis of what is euphemistically called “mere membership” in Communist or other extremist organizations.

The questioning of witnesses from the Civil Service Commission in public hearing established that, as matters now stand, the Civil Service Commission does not ask any applicants, even applicants for sensitive positions, whether they are or have been members of Communist or Nazi or other totalitarian or violence-prone organizations. Nor, in the absence of an overt violation of law, does the Commission, according to the witnesses, make an intelligence entry based on such information, if the information was provided by a third party. The list of organizations mentioned in the course of the questioning was a long one, but far from complete. It included the Communist Party, U.S.A., the KKK, the American Nazi Party, the Maoists, the Trotskyists, the Prairie Fire Organizing Committee which publicly supports the terrorist activities of the Weather Underground, the Puerto Rican Socialist Party which similarly supports and defends the actions of the Puerto Rican terrorists, the Jewish Defense League, and the Palestine Liberation Organization. The same answer apparently applied to all organizations: in the absence of an overt act, “mere membership” is not a bar to Federal employment.

The catastrophic plight of the Federal Employee Security Program was highlighted in a statement which the subcommittee received from two former Computer Security Evaluators (CSE) for the United States Army. Just before they retired from the Army there was an incident involving openings for three civilian Computer Security Specialists in a highly sensitive military computer operation. The function of a Computer Security Specialist is to protect computers against hostile penetration—surely a critical function, and one that should require a thorough background check and careful screening. But civilian positions in the Department of Defense fall under Civil Service Commission regulations—and in this case the instruction came down from the local Civilian Personnel Office that, even if an applicant was not clearable by Army standards, this fact could not be used to bar his employment as a Computer Security Specialist.

The sad state to which the Federal Employee Security Program has been reduced is also underscored by a number of items in a GAO report of November 15, 1978, prepared at my request. The report, entitled “Impact of the Freedom of Information and Privacy Acts on Law Enforcement Agencies,” included this item:

A recent Department of Justice applicant investigation developed a considerable amount of derogatory information. A U.S. district judge was interviewed, and he admitted that he had information which would bear on the investigation, but he refused to furnish it to the FBI because he said he knew that his information, once released outside the FBI, would not be protected to conceal him as the source of the information. He said other Federal judges felt the same way and believed that the Federal bench in general was unwilling to assist in such background investigations.

None of the witnesses who testified argued for the abolition of the Freedom of Information Act and the Privacy Act. All of them felt that the privacy legislation had much positive merit. All of them, too, conceded freely that there had been abuses in the past in the field of intelligence and that it was mandatory to have future intelligence activities governed by clear guidelines. The thrust of their argument was that a better balance had to be struck than is today the case between the right of privacy and the right to be secure—in one's person and in one's home and in one's property.

It should be cause for reflection that virtually no one in the media, no one in the Congress and no one in the Administration realizes just how far we have gone in stripping society of the ability to defend itself and defend its citizens, in consequence of the exaggerated and undiluted emphasis on privacy. It is noteworthy that the President's Privacy Protection Study Commission, after a one-year study, issued a 600-page report in which the entire concern was with ways and means of improving the quality of privacy—nowhere did the report manifest any concern over the erosion of law enforcement intelligence, or the breakdown of the one-time cooperative relationship between law enforcement and corporate security, or the inability of private corporations to do background checks on their employees, or the damage all this has done to the security of the individual and the security of society.

It is in the nature of new legislation that it is frequently impossible to predict its precise consequences and that it may be as much as four or five years before a reasonably accurate assessment can be made of its pluses and minuses. As often as not, new legislation has to be amended after such a trial period. I believe that the time has come for a re-examination of the privacy legislation now on the books and of the entire question of security in our society—from the security of nuclear installations to the security of the citizen in his home.

It is my hope that the body of evidence which has been brought together in this report will pave the way to an evenhanded discussion when the 96th Congress takes up the various recommendations of the President's Privacy Protection Study Commission. I believe this is not an unrealistic hope because a number of recent items in the press and several hearings conducted by other committees in the closing months of the 95th Congress suggest the beginning of a national awakening to the dangers which are the subject of this report.

During the three years of hearings which are here summarized, the press displayed an apparent indifference both to our hearings and to the entire subject of the erosion of law enforcement intelligence. But now things are beginning to change, and certain segments of the press are beginning to look into the situation on their own. Thus, a page one feature article in *The Washington Star* for August 29, 1978 spoke of "a growing trend by alleged organized crime figures to use the Freedom of Information Act and the Federal courts to get access to the investigative files the government has assembled over the years." The article quoted an unnamed FBI agent as saying "if the courts decide that we have to destroy or surrender all the material that we picked up on illegal taps, that could be just devastating." The article also noted that in one north central city at least 30 organized crime figures had filed FOI requests "in what appears to be a coordinated effort to learn what the bureau knows about their activities."

In a similar vein, the Wall Street Journal on September 27, 1978 ran an article headed "FBI Agents Rap Policy of Burning Files, Link to Public Access Acts." The article started out by telling the story of an extortion letter that was brought to the Detroit Field Office of the FBI for investigation. The style of the letter appeared to be similar to that of a man who had three years previously been investigated in connection with extortion threats. "Until recently," said the article, "agents could have pulled the suspect's file, done a quick check and perhaps protected the frightened citizen. This year, however, they couldn't. The file, like hundreds of thousands of other FBI files, had been destroyed under a policy that is reducing more than half the bureau's files to ashes." The article noted that under existing regulations files in auxiliary FBI offices are being burned after only six months, even though "so-called auxiliary offices often contain as much information as the files in the office of origin."

The awakening of the press has been paralleled by some probing questioning on the matters of law enforcement intelligence and the Federal Employee Security Program, in recent hearings before House and Senate committees. At a July 31, 1978 hearing of the Subcommittee on Evaluation, House Permanent Select Committee on Intelligence, Mr. Sebastian S. Mignosa, Chief of the Domestic Security Section, FBI, was asked whether his Section handled subversive organizations coming under the Loyalty and Security Program called for by Executive Order 10450. His reply was "we don't have any of those." When he was next asked who in the FBI dealt with such organizations, he replied: "There isn't any at the moment . . . There isn't any of those type cases at the moment."

In a subsequent hearing before the same subcommittee on September 19, 1978, Superintendent James E. O'Grady of the Chicago Police Department was asked why they have so little information about the Puerto Rican terrorist group, the FALN, which has claimed responsibility for the Fraunces Tavern bombing and many other bombings. His answer was that the Chicago Police Department was effectively foreclosed from gathering intelligence about the FALN "because anything that we learn at the present time regarding the FALN is open to inspection by the plaintiffs in the suit brought by the Alliance to End Repression, and what we put into our files would be made public shortly upon receipt of it."

I welcome these recent evidences that the press and Congress are becoming aware of the problem. It is, however, a problem with many aspects. It cannot be properly understood unless it is viewed whole, in all of its ramifications and complexities. The fact that criminals in large numbers are using the Freedom of Information Act for their own ends is only one small part of the much broader problem of the erosion of law enforcement intelligence and the zero security situation toward which this has been moving our society. The scope and depth of the report which follows will, I believe, help to give members of Congress a clearer perception of the total problem.

LIST OF HEARINGS AND WITNESSES COVERED IN THE FOLLOWING
REPORT

"The Nationwide Drive Against Law Enforcement Intelligence Operations"

July 11, 1975

James M. Rochford, Superintendent, Chicago Police Department.
Mitchell Ware, Deputy Superintendent, Chicago Police Department.
Eugene Dorneker, Investigator, Chicago Police Department.
Adelle Noren, Housewife, Chicago, Ill.
David Cushing, Police Officer, Chicago Police Department.

September 18, 1975

Francis J. McNamara, former Research Director and Staff Director of the House Committee on Un-American Activities (which later became the House Committee on Internal Security) and former Executive Secretary and Chief Clerk of the Subversive Activities Control Board.

"Terroristic Activity—Terrorist Bombings and Law Enforcement Intelligence"

October 28, 1975

Thomas G. Brodie, Bomb Specialist, Dade County Public Safety Department, Dade County, Fla.
Terence G. McTigue, Bomb Specialist, New York City Police Department.
Arleigh McCree, Bomb Specialist, Los Angeles Police Department.
Donald L. Hansen, Inspector, San Francisco Police Department.

"Threats to the Peaceful Observance of the Bicentennial"

June 18, 1976

Dr. William Kintner, President of the Foreign Policy Research Institute, Inc., of Philadelphia and Professor of Political Science of the University of Pennsylvania.
Inspector George Fendl, Philadelphia, Pa., Police Department.
Deputy Chief Robert L. Rabe, Metropolitan Police Department, Washington, D.C.

"The Erosion of Law Enforcement Intelligence and Its Impact on the Public Security"

July 13, 1977

Eugene Rossides, former Assistant Secretary of the Treasury for Law Enforcement.
John Olszewski, former Chief of Intelligence for the Internal Revenue Service.
Laurence Silberman, former Deputy Attorney General.

July 27, 1977

H. Stuart Knight, Director, U.S. Secret Service.

Glen D. King, Executive Director of the International Association of Chiefs of Police.

September 21, 1977

Peter Bensinger, Administrator, Drug Enforcement Administration, Department of Justice.

September 28, 1977

Donald R. Duckworth, Director of Corporate Security, Norton Co., Worcester, Mass., and Chairman, Privacy and Information Management Committee, American Society for Industrial Security.

Jan F. Larsen, Manager of Corporate Security, Pfizer, Inc., New York, N.Y.

Henry English, Secretary, Marine and Aviation Services, Insurance Co. of North America, Philadelphia, Pa., and Chairman, Transportation and Security Committee, American Society for Industrial Security.

Thomas F. Ruane, Jr., Corporate Manager of Security, Avon Products, Inc., New York, N.Y., and Regional Vice President, American Society for Industrial Security.

Lindsay L. Baird, Jr., Independent Security Consultant and National Chairman, Computer Security Committee, American Society for Industrial Security, Washington, D.C.

October 5, 1977

Robert E. Chasen, Commissioner of Customs, U.S. Customs Service.

Glenn R. Dickerson, Deputy Commissioner of Customs, U.S. Customs Service.

William Rosenblatt, Acting Director, Special Investigations Division, U.S. Customs Service.

Thaddeus Rojek, Acting Chief Counsel, U.S. Customs Service.

October 20, 1977

James M. H. Gregg, Acting Administrator, Law Enforcement Administration, Department of Justice.

February 9, 1978

Alan K. Campbell, Chairman, U.S. Civil Service Commission.

Robert J. Drummond, Jr., Director, Bureau of Personnel Investigations, U.S. Civil Service Commission.

February 28, 1978

Frank Carrington, Executive Director, Americans for Effective Law Enforcement, Inc., Evanston, Ill.

Charles E. Rice, Professor of Law, University of Notre Dame Law School.

March 9, 1978

Quinlan J. Shea, Director, Office of Privacy and Information Appeals, Office of the Deputy Attorney General, accompanied by Richard M. Rogers, Deputy Director, Office of Privacy and Information Appeals, Department of Justice.

April 25, 1978

William E. Williams, Deputy Commissioner, Internal Revenue Service.

S. B. Wolfe, Assistant Commissioner for Compliance, Internal Revenue Service.

Lester Stein, Deputy Chief Counsel—Technical, Internal Revenue Service.

April 27, 1978

E. J. Criscuoli, Jr., Executive Director, American Society for Industrial Security.

Robert B. Ross, Director of Security and Safety, Trinity Lutheran Hospital, Kansas City, Mo., and Chairman, Health Care Committee, American Society for Industrial Security.

Philip J. Cherico, Director, Security and Safety, Power Authority of the State of New York.

Clifford E. Evans, Director of Security, First Federal Savings & Loan Association of Wisconsin and Chairman, Banking and Finance Committee, American Society for Industrial Security.

Donald C. Drever, Director of Corporate Security, CNA Insurance Co., and National Chairman of White Collar Crime Committee, American Society for Industrial Security.

May 9, 1978

James M. Powell, Chief, U.S. Capitol Police.

Colonel Richard A. King, Chief, Police Department, Fairfax County, Va.

I. LAW ENFORCEMENT INTELLIGENCE: ITS NATURE AND ITS PURPOSE

In *Anderson v. Sills*, Chief Justice Weintraub of the New Jersey Supreme Court, affirmed that intelligence gathering was critical to government power, "to enable it to satisfy the very reason for its being—to protect the individual in his person and things."

In 1955, the Hoover Commission defined intelligence as that function dealing "with all things that should be known in advance of initiating a course of action." Chief Davis of the Los Angeles Police Department, who quoted this definition, made the observation that

without the ability to gather appropriate data, police administrators would be required to make major decisions regarding the deployment of personnel while realizing that they possessed mostly inadequate information . . . there are relatively few activities that can be assured of success when they are initiated without planning.

In an article he offered for the record, Chief Davis expanded on the Hoover Commission definition of law enforcement intelligence in a manner which underscored the preventive, or prophylactic, role of such intelligence. The article said:

Police operations can generally be viewed as either reactive or pro-active. The reactive approach is utilized when the officer responds to a situation without prior knowledge or information about a criminal act. After arrival, the officer prepares reports and attempts to gather information which might lead to the apprehension of the perpetrator. However, the event has already occurred and the police agency has failed to accomplish its primary objective of preventing crime.

The pro-active approach to police operations is gained through one of several processes, all categorized under the broad concept of intelligence. Generally, the intelligence function may be viewed as the systematic gathering and evaluation of data and the conversion of data into a usable form. Once the information has been accepted and properly evaluated, it may be disseminated to appropriate units or persons for the purpose of planning or preventing activities. There are two major intelligence categories: criminal intelligence, which relates directly to knowledge about individuals and organizations involved in or contemplating involvement in criminal activities; and public disorder intelligence, which relates to individuals or organizations which have threatened, attempted or performed illegal acts disruptive of the legally protected civil rights of citizens.

Mary C. Lawton, Deputy Assistant Attorney General of the United States, defined law enforcement intelligence in these terms:

Intelligence gathering involves the collection of information about individuals, their activities, and their planned activities, for the purpose of preventing or preparing to deal with threats to fundamental government interests or to individuals whom the government has a special duty to protect . . . (it is) undertaken to thwart certain activities rather than to prosecute.

Eugene Rossides, former Assistant Secretary of the Treasury in Charge of Law Enforcement, made the point that, in terms of its basic mode and purpose, law enforcement intelligence closely resembled the information-gathering process that characterizes the operations of all government departments and corporations. Said Mr. Rossides:

Look at any non-enforcement agency of the executive branch of the Government; look at the operations of every committee and subcommittee of the Congress; look at the business and professional community; and look at our educational and charitable organizations. You will see that intelligence gathering is essential to carrying on successfully their activities.

The nature of law enforcement intelligence, however, differs in one very important sense from the information-gathering process in non-law enforcement offices of government. In such offices the information required in the decisionmaking process is generally of a factual nature and lends itself to compilation by systematic research. Law enforcement intelligence, however, deals with the world of the secret and the devious. Criminals and terrorists and saboteurs and the fomentors of mass disorders do not notify the authorities of their planned activities. On the contrary, they seek to conceal both their identities and their general activities, employing a variety of stratagems.

Sometimes they will operate with false I.D.'s: testimony taken by the subcommittee in connection with its false I.D. legislation established that many criminal elements operate with multiple false I.D.'s. Sometimes they seek to conceal involvement in narcotics or other criminal operations by setting up legitimate businesses as covers. In the case of terrorists, they have in every country been able to escape apprehension and carry on their activities by moving from one "safe house" to another—provided by people who are generally sympathizers but not themselves terrorists. In general, all criminal elements seek to conceal themselves by blending into the community in one way or another.

In order to deal with such secret and frequently conspiratorial activities, the law enforcement community must be able to mount surveillance on those it has reason to suspect of criminal activity, must infiltrate its agents into criminal and extremist organizations, and must recruit informants ranging from prostitutes and underworld characters to public-spirited citizens motivated by a desire to serve their country. And in order to make a case, they must sometimes work for years, painstakingly compiling little bits and pieces of intelligence, gathered by their own agents and operatives and informants

or provided by cooperative law enforcement units or cooperative citizens.

First intelligence reports more often than not consist of "soft", or uncertain, intelligence, as opposed to "hard", or confirmed, intelligence. The soft intelligence may sometimes involve innocent people. It may lead nowhere. Or it may turn out to be completely worthless. But in many cases soft intelligence is the beginning of all intelligence, and it frequently leads to criminal convictions. Conversely, law enforcement intelligence would be gravely handicapped if it were ever made a rule that there had to be hard intelligence before a file could be opened.

Those who are in the business of law enforcement intelligence will frequently receive information from informants or from anonymous sources. At the point of receiving it, they have no way of knowing whether it is accurate—but the information has to be put on file and checked against other items of information that may in the future become available. By putting together a mosaic of many items of soft intelligence and perhaps only a few items of hard intelligence, it is frequently possible to establish as a fact that there is some criminal activity in the making or already perpetrated.

In the complex field of law enforcement intelligence, a single tiny and ostensibly unrelated item of information can sometimes frustrate a conspiracy or solve a major crime. Underscoring this point was a story related by Chief James M. Powell of the U.S. Capitol Police in his testimony of May 5, 1978. Chief Powell told the subcommittee about a letter he had received from an old friend in a local police department. The police department in question had some time previously instituted a central file on field interrogations and, as a result of this, they had been able to convict a murderer, despite an apparently fool-proof alibi. As Chief Powell told the story:

It seemed that a man wanted to do away with his wife and he got in a poker game and at the poker game he went to the men's room, and went out the window, and went home and killed his wife. He came back in through the window, and rejoined the poker game. Subsequently, when his wife was found, he had witnesses that at the time of the murder could testify that he was in a poker game. The only problem was that he ran a red light enroute back from having killed his wife, and he got a ticket. The police officer who gave him the ticket routinely put this in the central file for field interrogation. So when they routinely checked the master file as to what may have turned up, this man's name came up and showed that at the time he was, in fact, in his car enroute from having killed his wife.

After telling this story, Chief Powell commented that he was afraid he was "getting into an area that is frowned upon . . . by some groups. I am not sure that many police departments are able to keep the field interrogation systems anymore."

Obviously, because of its very sensitive nature, law enforcement intelligence must be guided by carefully drawn criteria and directed by expertly trained officers who are knowledgeable about the law and sensitive to the requirements of privacy. As Mr. John Olszewski,

former Director of Intelligence for the Internal Revenue Service, told the subcommittee:

It is essential for police departments and other law enforcement agencies to avoid excesses, bad judgment, overzealousness, and any semblance of unnecessary and unwarranted intrusions into the privacy of the law-abiding citizen.

As a matter of fact, an information-gathering system which is not specifically directed to the criminal, his associates, and his activity is doomed to failure. It will simply be unmanageable, overburdened with irrelevant data, and valuable information about true criminals is likely to be lost and become irretrievable.

Obviously, too, intelligence files must be reviewed and purged periodically in order to eliminate worthless and irrelevant information. A regular and systematic pruning of the files is essential for an efficient intelligence operation. But there is a serious danger in establishing short term arbitrary deadlines of, say, 2 to 3 or 4 years, requiring the closing out of files if they cannot by that time be converted into court cases. The fact is that first entries in intelligence files may remain unsupported for long periods of time or—which happens more frequently—the additional information that comes in over the first several years may still be insufficient to bring the case to court. This point was emphasized by a number of the witnesses before the Subcommittee. Mr. Olszewski put the matter thus:

Information about members of these criminal groups at every level is essential to effective law enforcement today, tomorrow, and even years from now. A low-level member of a loanshark syndicate in Chicago, Detroit, or New York may be tomorrow's upper echelon syndicate leader in Las Vegas or Miami.

For example, a major racket figure, said to be currently under investigation in the West, 7 years ago was a midlevel strong-arm man in the Midwest. His background, former contacts, and associates are important factors in today's investigation. Unless this background information over the years is maintained—retained—and is legally available, investigations will be unnecessarily prolonged and are likely to be unsuccessful. Thus, it is the public interest which suffers.

How does one strike a balance between the need to keep intelligence on file as long as there is a reasonable chance that it may serve a purpose at a later date, and the need—in the interest of privacy as well as in the interest of sound intelligence procedures—to periodically purge intelligence files of irrelevant and useless information? Certainly there is no point in keeping information on file for 20 or 30 years if the file remains inactive after one or several inconclusive entries.

The matter calls for careful evaluation by experts in the field of intelligence, rather than for arbitrary deadlines imposed by privacy enthusiasts who have no practical understanding of the workings of law enforcement intelligence or of the vital importance of law enforcement intelligence in protecting society and in protecting the individual. Conceivably, a balance might be struck by requiring a review of all intelligence files that have not yet been converted into court cases 10 years after they are opened.

Whatever guidelines may finally be decided on governing the retention of law enforcement intelligence, the importance of continuity cannot be overstressed.-As Mr. Olszewski stated the matter:

Enforcement of laws against the well-organized continuing illegal activities of crime syndicates requires general intelligence gathering on a continuous and long term basis. It cannot be turned on and off like a faucet. Any significant break in the continuity and consistency in quality of the flow of information can seriously jeopardize and doom to failure any planned law enforcement program against the organized or syndicated entrepreneurs.

Beyond the need for continuity, there is the need for sharing of intelligence. This was a matter to which many of the law enforcement witnesses addressed themselves. Again, to quote Mr. Olszewski:

Failure to provide for the legal sharing of intelligence between police and law enforcement agencies about suspect backgrounds, methods of operations, suspect associates and surveillance data, can only result in a drop in effectiveness of law enforcement, continued erosion of the safety and security of the general public. Finally, a demand by law enforcement administrators for more manpower to compensate for their drop in effectiveness.

Without a well-planned, effective and continuing intelligence-gathering program for syndicated criminal investigations, the problems for the investigators are gigantic.

Without the ability to freely query other law enforcement agencies and to legally share basic background information about persons engaged in syndicated or organized criminal activities, law enforcement is literally "hog tied".

One of the many purposes of law enforcement intelligence has to do with the protection of communities against the kind of mass violence and mass disorders that erupted in many of our cities in the late 1960's and early 1970's. The so-called Kerner Commission (National Advisory Commission on Civil Disorders) which was set up for the purpose of looking into the causes and nature of these disorders, methods of containing them, and more durable solutions, placed heavy emphasis on the need for effective police intelligence—

To aid in the evaluation and determination of the probability of unlawful disorders, large-scale violence, and potential riots;

To aid in the determination of supplemental police manpower needs;

To facilitate decisions and planning for coping with disorders anticipated or in progress;

To aid in familiarization with the past activities of professional agitators, their tactics and control over their followings; and

To furnish information for meetings of the Governor with officials of various State Departments . . . so that this information can be used by the Governor and appropriate governmental agencies to alleviate present tensions and prevent future and potential disorder.

There can be no question but that law enforcement is crippled when it is stripped of the intelligence function, nor can there be any question that, in hundreds and thousands of instances, it has served to frustrate

criminal conspiracies, obtain criminal convictions, and protect the community against mass violence and threatened disorders. Mr. Frank Carrington, in his testimony before the subcommittee, submitted as an exhibit a copy of a brochure, entitled "The Defenseless Society," which he had co-authored under the auspices of Americans for Effective Law Enforcement. The brochure contained a long list of specific instances where effective law enforcement intelligence had served to protect communities in various parts of the United States. Since it would be difficult to improve on these very succinct summaries, a few of them are reproduced in the paragraphs that follow as they appeared in "The Defenseless Society":

The Deep South: Early 1960's

Through extensive use of informants, infiltration, surveillance, and the exchange of information, the FBI brought the Ku Klux Klan and other racist groups to their knees, breaking their reign of terror directed against Negroes and white civil rights workers.

Boston, Mass.: 1974-75

This city became embroiled in one of the worst controversies over school busing that this nation has ever seen. Commissioner Robert DiGrazia of the Boston Police Department writes of the intelligence activities which helped his department to minimize violence to the extent possible:

"(a) Since June of 1974, intelligence gathering efforts have been directed toward the school busing problem that is currently plaguing the City of Boston. Demonstrations taking place at various times throughout the City by anti-busing and pro-busing forces have been accurately forecast by Intelligence Division personnel. These reports are used by our Operations Section to deploy the manpower used to cope with the crowd control and traffic problems resulting from demonstrations and motorcades of hundreds of cars.

"(b) In December of 1974, a plot to bomb bridges was discovered by intelligence sources cooperating with other law enforcement agencies and publication of the plot has deterred the people involved from carrying through on the proposed disruption of traffic over major arteries in this City. Subject matter is still under active investigation."

Organized crime

(a) A son of a Mafia leader was known to local area organized crime investigators prior to his arrival in this area in the early 1950's. Forearmed with this intelligence information regarding his known Mafia and organized crime associations, his activities in this area were periodically monitored. Over a period of years, these periodic checks revealed a pattern of associations with other known organized crime figures in the area.

These observations indicated the need for a more intensive investigation of possible criminal activities on his part. Organized Crime Intelligence investigators produced information which was felt sufficient to warrant investigation

of specific criminal activity in the areas of narcotics violations, gambling, racketeering, loansharking, and extortion.

Using this information, investigators produced evidence which resulted in federal indictments, first for narcotics smuggling and gambling in January, 1974, and subsequently for racketeering, loansharking, and extortion in July, 1974. These indictments resulted in his conviction along with several associates, on these charges in September, 1974.

* * * * *

Riots

(c) During the years 1965 through 1973, a period during which our country bore witness to acts of civil turmoil and disruption, California campuses and universities became the proving grounds for many guerrilla policies and tactics. Nationwide violence was rapidly replacing the peace, decorum, and tranquility that had long been part of academia. It became incumbent upon law enforcement to determine all that contributed, combined, or constituted each act of violence or destruction. In the early part of 1970, UC-Santa Barbara fell prey to one of the greatest, longest campus disturbances in U.S. history. Countless injuries and even death were suffered by students, civilians, and law enforcement officers alike. Banks were burned and property destruction was extensive. The riot had continued for three months.

Based on a mutual aid pact, the smaller Santa Barbara area law enforcement agencies requested assistance from Los Angeles County Sheriff's Department; intelligence operations already underway were increased extensively. Using undercover intelligence officers, informants and techniques, the tactical plans of the now greatly increased law enforcement team advanced on the problem situation. Riot ring leaders were quickly identified and removed. Advance plans of the rioters were suddenly nullified or failed. The three-month riot was over in three days with the injuries and property damage immediately reduced. As ring leaders were identified and nullified, the hard core offenders, many of them non-students, left the area and the state. Life returned to normal in Santa Barbara.

San Diego, Calif.: 1971-75

The San Diego Police Department reported the following five cases of the use of intelligence gathering techniques:

(a) On March 28, 1971, a leftist organization known as the People's Peace Treaty held a march and rally in Ocean Beach protesting the construction of apartment buildings at Collier Park. Approximately 300 people were involved in the demonstration, which became a riot after the participants caused disturbances and destroyed property in the area of the park.

Approximately 100 uniformed officers attempted to quell the riot after it was declared an unlawful assembly. During the riot, one officer was struck in the eye by a thrown rock and lost the sight of his left eye. Another officer was badly beaten and cut and received serious injury at the hands of a demonstrator wielding a shovel.

Fifty-six persons were arrested for charges such as possession of narcotics, disturbing the peace, unlawful assembly and failure to disperse. Nine persons of the fifty-six arrested were charged with felonies for assaulting uniformed officers with deadly weapons. Those persons charged with felonies were identified by Intelligence officers who were surveilling the entire incident. In those nine felony cases the criminals would probably have remained anonymous and would not have been recognized by uniformed officers who were involved in suppressing the riot.

* * * * *

Right-wing extremists

During 1972 a major case dealt with the members of the Secret Army Organization, an ultra right-wing activist group which bombed a local theater and attempted the murder of a political adversary in Ocean Beach. This four-month investigation conducted by the Intelligence Unit caused the service of six search warrants, the seizure of automatic weapons, explosives, and illegal military drugs, the arrest and conviction of eight Secret Army Organization members and associates for charges ranging from attempted murder to perjury, and the total destruction of the Secret Army Organization in the western states. Due to the wide range of violations and the geographical area, the Federal Bureau of Investigation, the Alcohol, Tobacco and Firearms agency, the San Diego Sheriff's Office and the El Cajon Police Department were utilized for assistance. This case also required 24-hour protection for an informant and his family and, later, his relocation to a different jurisdiction.

THE IMPORTANCE OF INTELLIGENCE AS VIEWED BY NATIONAL COMMISSIONS

Mr. Francis J. McNamara, former Executive Director of the Subversive Activities Control Board, pointed out in his testimony of September 18, 1975, that at least seven U.S. national commissions had underscored the importance of intelligence in dealing with organized crime as well as civil disorders. These commissions were:

The Commission on the Assassination of John F. Kennedy, which was appointed by President Johnson on November 29, 1963, and which issued its report on September 24, 1964.

The President's Commission on Crime in the District of Columbia, set up by President Johnson in July 1965.

The President's Commission on Law Enforcement and the Administration of Justice, set up by President Johnson in 1967 under the chairmanship of former Attorney General Nicholas deB. Katzenbach.

The National Advisory Commission on Civil Disorders, appointed by President Johnson on July 29, 1967.

The National Commission on the Causes and Prevention of Violence, which was appointed by President Johnson in June 1968 and had its life extended by President Nixon to May 1969.

The President's Commission on Campus Unrest, appointed by President Nixon on June 30, 1970.

The National Advisory Commission on Criminal Justice Standards and Goals, appointed on October 20, 1971, by President Nixon.

Mr. McNamara quoted excerpts from the reports of all of these national commissions on the specific subject of law enforcement intelligence.

He quoted the report of the President's Commission on the Assassination of John F. Kennedy, as follows:

The Commission recommends that the Secret Service completely overhaul its facilities devoted to the advance detection of potential threats against the President.

* * * * *

The Commission recommends that the Secret Service continue its recent efforts to improve and formalize its relations with local police departments in areas to be visited by the President.

Mr. McNamara noted, in connection with these recommendations, that Lynette Fromme, Arthur Bremer, Sirhan Sirhan, and Lee Harvey Oswald were all political activists.

The President's Commission on Crime in the District of Columbia, Mr. McNamara recounted, employed the International Association of Chiefs of Police (IACP) to make an in-depth study of the District of Columbia Police Department. The 450-page report submitted by the IACP to the Commission was highly critical of the District of Columbia Police Department, especially of its lack of an intelligence unit. It recommended the establishment of a 14-man intelligence division, divided into 3 sections—subversives, organized crime and rackets. On the subject of the function of the Subversives Intelligence Section, the IACP report said:

This section is responsible for collection and appropriate dissemination of information about groups and individuals that threaten the security of national and local government. Members should develop information concerning structure, membership, and plans of organizations engaged in subversive activities, including those which have the intent to create religious and racial prejudices and those which advocate disturbances and violence.

Pursuant to this report, it should be noted, a Domestic Intelligence Unit was set up by the District of Columbia Police Department. This unit, which performed extremely well in dealing with the difficult disorders of the late 1960's and the early 1970's, was put out of business in 1975 pursuant to a resolution of the District of Columbia City Council.

The President's Commission on Law Enforcement and the Administration of Justice, in its 1967 report, said:

Procedures for the acquisition and channeling of intelligence must be established so that information is centralized and disseminated to those who need it.

On the specific subject of organized crime, the report said:

Much of the information in intelligence unit files on individuals relates to organized crime's "legitimate" business enterprises, meeting places, personal data, and other information which may be widely disseminated.

The Commission also recommended, noted Mr. McNamara, that the Federal Government create a centralized computer index into which all Federal agencies would feed information.

The National Advisory Commission on Civil Disorders submitted its report on March 1, 1968. Mr. McNamara quoted the following paragraph from the report's "Supplement on the Control of Disorder":

Intelligence—The absence of accurate information both before and during a disorder has created special control problems for police. Police departments must develop means to obtain adequate intelligence for planning purposes, as well as on-the-scene information for use in police operations during a disorder.

An intelligence unit staffed with full-time personnel should be established to gather, evaluate, analyze, and disseminate information on potential as well as actual civil disorders. It should provide police administrators and commanders with reliable information essential for assessment and decision-making. It should use undercover police personnel and informants but it should also draw on community leaders, agencies, and organizations in the ghetto.

Paralleling these recommendations, the report put out by the National Commission on the Causes and Prevention of Violence in December 1969, stated:

We urge police departments throughout the nation to improve their preparations for anticipating, preventing and controlling group disorders.

* * * * *

A major weakness of many police departments is the absence of a reliable intelligence system. This absence has gravely handicapped police and public officials in anticipating and preventing trouble, and in minimizing and controlling a disorder that has broken out.

Noting that intelligence had improved on the Federal and local level, the Commission's report nevertheless warned:

. . . we must anticipate other acts of lawlessness and terrorism to occur in various parts of our country which the radical extremists on both sides will try to exploit to their own advantage and objective. The immediate security pro-

blem will require necessary measures that will enable the police and civil authorities to distinguish among those who seriously wish violently to disrupt, those who engage in disruptive conduct out of fear and frustration, and those who wish to participate in peaceful protest and demonstration.

A critical ingredient to the success and effectiveness in coping with these control problems is good intelligence. It is essential that the police possess an intelligence system which enables them to measure with precision the real threat to the community posed by individuals and groups.

In discussing the role of intelligence in dealing with campus disorders, the President's Commission on Campus Unrest said in its report of 1970:

. . . If the police are to do their job of law enforcement on the campus properly, they need accurate, up-to-date information. Only if they are well informed can the police know how and when to react and, equally important, when not to react.

* * * * *

. . . It is an undoubted fact that on some campuses there are men and women who plot, all too often successfully, to burn and bomb, and sometimes to maim and kill. The police must attempt to determine whether or not such a plot is in progress, and if it is, they must attempt to thwart it. If they are unable to prevent it, they must seek to identify, locate, and apprehend the participants after the fact. The best, and sometimes the only, means the police have to effect these purposes, especially the preventive one, is by clandestine intelligence work.

* * * * *

Police cannot be barred from university campuses. The police are dutybound to enforce the law on the campus as well as elsewhere within their jurisdiction. When there is personal injury or serious property damage on the campus, the police must enforce the criminal law.

The university has no capacity to deal with bombing, arson, and similar acts of violence or terrorism. It must call the police. Such criminal acts put the entire community in such obvious and immediate danger that the police are obliged not only to discover their perpetrators, but also to take all reasonable steps to prevent their occurrence.

Finally, Mr. McNamara quoted the following passage from the January 1973 report of the National Advisory Commission on Criminal Justice Standards and Goals:

Every police agency and every State immediately should establish and maintain the capability to gather and evaluate information and to disseminate intelligence in a manner which protects every individual's right to privacy, while it curtails organized crime and public disorder.

Summarizing the findings, recommendations and standards, proposed by the seven national commissions, Mr. McNamara underscored the fact that this work represented—

... almost 9 years of concentrated study by hundreds of highly qualified persons who served as commission members, advisors, consultants and staff—leaders from all levels of government; the clergy, doctors, psychologists, historians, sociologists, lawyers, prosecutors, psychiatrists, as well as professional law enforcement personnel. Just about every intellectual discipline, every field of learning was represented on these commissions. Their work product represents—I think we can say—the best thinking available to this Nation on police operations and it is highly significant that they were unanimous and unqualified in their endorsement of police intelligence activity, including intelligence in the so-called political area.

The recommendations of the seven national commissions which have been quoted in the preceding section, have, regrettably, produced no meaningful reaction at the Federal, State, or local level. On the contrary, in a blind reaction to Watergate and the admitted excesses in intelligence activities that have been brought to light since Watergate, the nationwide tendency has been to do precisely the converse of what the seven national commissions recommended in the field of law enforcement intelligence. The capabilities of our law enforcement organizations, in consequence, have been cumulatively undermined for almost a decade now. In many situations, their intelligence capabilities have been reduced to the point where they are compelled to play a game of blind man's bluff. As the testimony summarized in the following pages establishes, it is the American people who are the ultimate victims when the law enforcement community, as a result of its reduced intelligence capabilities, is less able to protect them against the operations of organized crime, the ominous and growing danger of terrorist activity, the long term threats posed by organized subversion, and the always unpredictable possibilities of new civil disorders.

This creates a frustrating situation for our law enforcement agencies. Beyond that, it places them in an invidious position.

In the past, when they had quality intelligence, they were able to deal with mass demonstrations with a minimum show of force and they were able to defuse disorders rapidly because they knew who the ring-leaders were and they knew a good deal about their plans. Today, without such information, law enforcement agencies are repeatedly confronted by the dilemma of how much manpower to provide. The temptation is to throw in more manpower in order to plug the intelligence gaps. If they do so, however, as Chief Powell of the U.S. Capitol Police told the Subcommittee, they are frequently criticized for engaging in an excessive show of force or for over-reacting. Conversely, if they fail to anticipate disorders and provide inadequate manpower they are criticized for failing to make adequate preparations—as was the case when Iranian student extremists got out-of-hand during the recent visit of the Shah of Iran to the White House.

Stuart Knight, Director of the Secret Service, testified that his own agency was confronted with a similar Catch-22 situation. On the one hand, the Secret Service and the various law enforcement agencies which provide it with intelligence are under continuing criticism for engaging in excessive surveillance of radical and extremist elements. On the other hand, if a Lynette Fromme or a Sara Jane Moore tries to assassinate the President, the cry immediately goes up: "Why did the Secret Service fail to identify these extremist or psychotic elements and take preventive action against them?"

II. FACTORS CONTRIBUTING TO THE EROSION OF LAW ENFORCEMENT INTELLIGENCE

The first hearings on the erosion of law enforcement intelligence were held in mid-1975 by the Subcommittee on Internal Security (which was incorporated into the Subcommittee on Criminal Laws and Procedures in July 1977). At the time it embarked on these hearings, the subcommittee was aware that there had been a serious erosion of intelligence and a general downgrading of intelligence activities, but it was under the impression that the erosion had to do primarily with intelligence on terrorist and subversive organizations. It did not realize at the time—this was developed only in the course of the hearings—how pervasive the erosion was and how much damage had been done to the overall ability of the various Federal, State, and local law enforcement agencies to guarantee the security of Government, of private corporations, and of the public generally.

The subcommittee's early perception of the problem was reflected in the opening statement made by Senator Strom Thurmond, who presided at the hearing of September 18, 1975:

The Senate Internal Security Subcommittee has received information from sources in many parts of the country pointing to the conclusion that there has been a highly organized and highly effective drive, on a national scale, against law enforcement intelligence operations. The scale of the operation may be gleaned from the fact that some 75 separate suits have been filed against law enforcement agencies, ranging from the FBI to the local police departments, seeking to compel them to divulge sensitive intelligence gathered on extremist groups, or to divest themselves entirely of their intelligence files and intelligence operations.

The legal harassment has been compounded by the apparent willingness of many people in our media to regard our law enforcement agencies as the prime enemy of our freedoms rather than as their protector, and to disregard or minimize the danger posed to our freedoms by the scores of extremist organizations openly committed to terrorist activities or to the violent overthrow of our form of government.

* * * * *

Unsure of their own rights, and understandably fearful that they might be found in violation of the Constitution, and anxious to disengage from the pressure of legal harassment, some of our law enforcement agencies have completely disbanded the special intelligence units they previously maintained to monitor extremist groups of the left and right, while other law enforcement agencies have destroyed the intelligence files laboriously built up through many years of effort.

* * * * *

I do not say that there have not been excesses and errors by our law enforcement intelligence units. The scale of the operation, nationally, would make a small quota of errors in judgment almost unavoidable. But the answer to such errors is not the abolition of our law enforcement intelligence files and law enforcement intelligence units—this would invite the destruction of our society. The answer lies, rather, in establishing carefully defined standards governing the operations of law enforcement intelligence, so that the officers involved will know what kinds of organizations and individuals require surveillance, and what methods are proper and what methods improper.

We have to strike a balance between protecting our constitutional liberties and protecting our society against those who would destroy it. On this point, I concur in the wise opinion expressed by former Supreme Court Justice Jackson some time before his death:

"The Court's day-to-day task is to reject as false, claims in the name of civil liberty which, if granted, would paralyze or impair authority to defend the existence of our society, and to reject as false claims in the name of security which would undermine our freedoms and open the way to oppression."

As the hearings proceeded, it soon became evident (1) that the erosion was not limited to political intelligence activities—that ordinary criminal intelligence, including intelligence on organized crime, had also been seriously crippled; (2) that the erosion was so pervasive that it affected the personal security of every citizen; (3) that every law enforcement agency in the country from the Federal to local level had been adversely affected, and (4) that the factors contributing to the erosion of law enforcement intelligence were substantially more complex than the subcommittee had originally perceived them.

The testimony of the numerous witnesses who appeared provided ample and dramatic confirmation of the role played by the three factors mentioned by Senator Thurmond in the opening statement quoted above—that is, the negative attitude of the media, legal harassment by left-wing organizations, and the widespread uncertainty in the law enforcement community over what was permissible and what was not permissible.

Backtracking somewhat, one would have to include in the list of contributing factors the widespread bias against intelligence in the post-Watergate period, resulting from the revelation of some very real abuses. One would also have to include, as an early contributing factor, the understandable concern on the part of many citizens that the massive quantities of personal data on file in the Nation's numerous computer systems called for more stringent laws to protect the privacy of the individual. These concerns provided the primary private and political justifications for the Privacy Act of 1974 and for the sweeping amendments in the same year to the Freedom of Information Act. It is noteworthy that all of the law enforcement officers and officials of law enforcement agencies who testified before the Subcommittee stressed the major role played by both the Privacy Act and the amended Freedom of Information Act, and by parallel legislation at the State level, in the erosion of their intelligence capabilities.

There was also general agreement that uncertainty about the various laws in the field of privacy was having a paralyzing effect on law enforcement agencies and private security, which manifested itself in self-imposed restrictions not actually required by the law.

The paragraphs that follow summarize in more detail the various factors contributing to the erosion of law enforcement intelligence, as they were described to the subcommittee by its numerous witnesses.

THE ROLE OF THE MEDIA

Mr. Glen King, executive director of the International Association of Chiefs of Police (IACP), described to the subcommittee the highly adverse affects which the generally negative attitude of the media was having on law enforcement. His testimony on this point is crystallized in the following paragraphs:

The media can have a substantial effect upon a law enforcement agency's intelligence operations in that the press can direct an agency's attention from intelligence activities to answering harassing, and oftentimes invalid charges. The demoralizing effect upon an intelligence unit's personnel is all too readily understood. Furthermore, press leaks concerning ongoing intelligence operations, whether true or false, may jeopardize the effectiveness of surveillance in that it may warn those individuals or groups who are the subjects of the surveillance.

The Arlington, Tex., police force has been challenged by the press as to the need for intelligence surveillance on a local university campus. This reporting may very well have compromised this surveillance.

The Seattle Police Department often finds itself in the position of being judged by the media as to whether it was proper for the department to conduct certain intelligence-gathering operations.

As I previously stated, the Chicago intelligence unit is being adversely affected by information being published as a result of the pending suit.

As a result of the electric atmosphere surrounding all intelligence operations, a great loss of effectiveness has occurred. State and local law enforcement officials are keenly aware of the FOIA and Privacy Act and their effects on State and local intelligence operations.

Capt. Justin Dintino, chief of intelligence of the New Jersey State Police, estimated that about 90 to 95 percent of the articles having to do with law enforcement in the New Jersey press were derogatory. In one instance, he said, a leading newspaper in the State of New Jersey did a series of articles on the State police intelligence bureau in which they raised the specters of secret files and political dossiers and of the unauthorized dissemination of information and the absence of guidelines. Captain Dintino made the point that, in doing this story, the newspaper in question made no effort to obtain information from any responsible officer of the intelligence bureau. The articles, he said, were based on hearsay and rumor.

I would have welcomed the opportunity to take him (the reporter) through my bureau, show him our guidelines, and show him exactly what kind of files we do maintain. We were doing nothing in secret. We published our guidelines, as far as we made them public.

Captain Dintino said that the series of articles in question led to the passage of a resolution by the State legislature calling for an examination of State police intelligence files and of their entire intelligence methodology and guidelines. Pursuant to this, a State investigative commission was set up, which, after about 7 months' work, concluded that there was no need to conduct an in-depth investigation. "But all during this time period," said Captain Dintino, "you can imagine the chilling effect that it had on my operation and on my people, morale-wise."

Mr. Francis J. McNamara, former executive secretary of the Subversives Activities Control Board, who testified on September 18, 1975, told the subcommittee about a similar situation in the city of Baltimore the previous year. As a result of a lengthy series of articles in the Baltimore press, alleging abuses by those responsible for police intelligence operations, a grand jury was impanelled to conduct an investigation of the charges. "The prosecutor who handled the grand jury," said Mr. McNamara, "made a statement after it had been in session for over a period of 4 or 5 months—he stated that in all of these proceedings the grand jury had not been able to find one iota of evidence that the police intelligence squad had done anything illegal."

Mr. J. Phillip Kruse, special agent in charge of the intelligence unit of the Illinois Bureau of Investigation, concurred with Captain Dintino's estimate that the substantial majority of media articles dealing with the subject of law enforcement intelligence were generally critical. He said his bureau had been "the subject of a great number of sensational headlines in recent months and a front-page article, which was later retracted." Referring specifically to the case of the Chicago Police Department, which had been under even greater pressure from the media, Mr. Kruse said: "I am sure that Jim Rochford [superintendent of the Chicago Police Department] didn't coin the phrase 'Chicago Police Spying'." [The case of the Chicago Police Department will be dealt with separately and at greater length at the conclusion of this section.]

ORGANIZED LEGAL HARASSMENT

The erosion of law enforcement intelligence has not been entirely the product of a spontaneous popular reaction to the excesses revealed by the Watergate crisis, or of the growing concern over the impact of computer systems on personal privacy, or of the generally negative attitude of the media. An important role in the erosion has been played by a highly organized campaign launched in the early 1970's with the declared purpose of wiping out law enforcement intelligence activities.

Speaking about this matter, Senator Thurmond said, in his opening remarks, at the hearing of September 18, 1975:

The organizations of the far left, needless to say, have been major and enthusiastic participants in the national drive against law enforcement intelligence. In this, regretfully,

they have been abetted by organizations and individuals whose primary concern is the protection of civil liberties. For example, the American Civil Liberties Union, which has been instrumental in the filing of some 30-odd suits against local, State, and Federal enforcement authorities, had this to say in its 1970-71 annual report:

"The ACLU has made the dissolution of the Nation's vast surveillance network a top priority. . . . The ACLU's attack on the political surveillance is being pressed simultaneously through a research project, litigation, and legislative action."

Senator Thurmond's statement received powerful confirmation from the testimony of Mr. McNamara and the Chicago Police Department.

Mr. McNamara testified that the American Civil Liberties Union (ACLU), in a recent article on surveillance, referred to 75 suits by "civil liberties" lawyers. Some of these suits were brought by the ACLU itself, some were brought by the National Lawyers Guild (NLG), and some by the Law Center for Constitutional Rights.

Mr. McNamara noted that the National Lawyers Guild had been characterized 25 years ago by the House Committee on Un-American Activities as the "foremost legal bulwark of the Communist Party" and its unions and fronts in this country. Since this characterization was made, he said, its composition has changed somewhat in the sense that it now includes a lot of New Left radical lawyers, in addition to the old-line Communist Party members. He pointed out that "Guild Notes", an official publication of the Guild, for July 1975, printed an article advocating revolutionary armed struggle in U.S. prisons. This article stated at one point:

. . . Many people within the Guild consider the strategy of armed struggle to be an integral part of any revolutionary struggle . . . the Guild must make room for those who believe in revolution and armed struggle.

The Law Center for Constitutional Rights, testified Mr. McNamara, is an offshoot of the National Lawyers Guild. It was organized by William Kunstler, Arthur Kinoy, and Mort Stavis. In the case of Mr. Kinoy, Mr. McNamara offered the following information:

I might point out that Mr. Kinoy, who teaches constitutional law at Rutgers, was on some of these suits. He is a leader and principal organizer of a new group called the National Interim Committee for a Mass Party of the People, and this group is coming out as being openly revolutionary. It is an attempt to create a new Marxist-Leninist Party in this country—openly Marxist-Leninist—which would be to the left of the Communist Party itself. This group, usually referred to as the "NIC," says that the Chinese, Cuban and Vietnamese revolutions inspire its thinking and strategy, that it stands for "the transfer of power from the capitalist state and corporations to the people" and that the United States is the "main enemy of millions of people engaged in life and death struggles from one end of the globe to the other."

As the testimony on the Chicago Police Department establishes, the Alliance to End Repression, whose suit against the Chicago Police Department has virtually destroyed its intelligence capabilities, is headed by men who have been identified as Communists or who have long records of Communist associations.

The ACLU enjoys somewhat of a national reputation as a non-partisan group concerned with civil liberties. Mr. McNamara noted, however, that in pressing all of its suits against law enforcement intelligence, the ACLU "is tying up with Communists, radicals, openly revolutionary groups, to destroy the ability of the United States Government on all levels to protect the people from terrorism and other subversive activities."

He further noted that Frank Donner, who had been identified in the 1971-1972 ACLU Annual Report as Research Director of the ACLU Political Surveillance Project, had served as counsel for the United Electrical Workers Union, which had been expelled from the CIO on grounds of Communist domination, and that he had three times been identified as a Communist in sworn statements before the House Committee on Un-American Activities.

The organized nationwide campaign of legal harassment against law enforcement agencies, in addition to crippling intelligence activities, has damaged the entire fabric of law enforcement in many other ways. Mr. Glen King, of the IACP, told the subcommittee that: "The time and expense incurred in answering inquiries and preparing for litigation are astronomical. In addition, such expenditures cut into the time and money which would normally be used for intelligence purposes." Mr. King illustrated his statement by providing brief summaries of the legal actions and other harassments that police departments have had to contend with in different parts of the country. The following paragraphs are excerpted from his summary:

In Dade County, Fla., for example, the public safety department has been subjected to two lawsuits within the last year in which the plaintiffs sought access to their intelligence files in the midst of an ongoing police investigation.

The St. Louis Police Department has been subject to litigation to obtain intelligence files. The Church of Scientology, the Socialist Worker's Party, and the ACLU have attempted through litigation or via subpoenas in other suits to gain access to intelligence data and files.

The Seattle, Wash., Police Department is currently being subjected to two lawsuits requesting access to intelligence information. In one of the pending cases, the Church of Scientology has requested access to files containing confidential information supplied by the Los Angeles Police Department that was gathered during an investigation of the church. The other suit has developed via a joinder of claims in which the ACLU, the American Friends Service Committee, the National Lawyers Guild, Coalition Against Government Spying, and others are seeking to obtain intelligence files. This same coalition of groups has sponsored a seminar for private individuals instructing them on the methods of obtaining law enforcement intelligence files. As a result, the department has been the target of approximately

60 letters from private citizens requesting disclosure of their respective files. These requests were undertaken notwithstanding a State public disclosure law which exempts intelligence files from disclosure.

The Arizona Department of Public Safety has been faced with a more serious problem. Within the last 2 years, the department has been subject to four subpoenas for the release of intelligence files to be used in other litigation. To date, the department has been protected from disclosure of these files following an *in camera* inspection. Requests such as these arise because Arizona has no statute that exempts intelligence files from public access.

The department has not been the subject of direct lawsuits. These subpoenas have arisen out of third party civil suits; for example, an organized crime figure sued his employer for defamation, the result of information which he complained was derived from an intelligence file maintained by the department. He, therefore, subpoenaed the file to prove his claim.

The department does, however, face the danger of having to provide access to the intelligence files if a case ever reaches the Arizona Supreme Court. The court through prior comment has indicated that, if it were to rule on the issue of access to police intelligence files, it would consider them public records on the basis that there is lacking a State law which exempts their disclosure.

The court's comment was a "side bar" comment, made off the record, pertaining to another case involving investigative files, on which it declined jurisdiction.

The Michigan office of the attorney general has stated that courts have ordered intelligence files impounded. The locking up, or impounding, of files may render past intelligence efforts fruitless, as well as the future use of the files impossible. The use of these files even for background checks for prospective employers is impossible if said files are impounded or locked up.

Needless to say, the relentless legal harassment of law enforcement agencies and law enforcement officers has had a highly demoralizing effect. Mr. John Olszewski, former Director of Intelligence for the IRS, told the subcommittee that it was "creating a serious climate of fear". He went on to say:

Law enforcement officers are not people of means. As a result, many are taking one of three courses of action—

1. They are attempting to buy personal liability insurance, or
2. They are avoiding involvement in duties which may make them vulnerable.
3. If assigned these duties, some will simply avoid inputting data into the record.

To this sorry state has law enforcement now been reduced. It should be evident that unless some way can be found of turning the situation around, the American people will simply have to live with the fact that their local police departments and other law enforce-

ment agencies cannot protect them as effectively as they would like them to do.

CHICAGO: A CASE HISTORY

Chicago provides a dramatic example of how a cleverly orchestrated campaign by a militant left-wing organization can paralyze the domestic intelligence operations of a major metropolitan police department. This was the subject of an executive hearing conducted by the Senate Subcommittee on Internal Security in July of 1975.

The witnesses included James M. Rochford, superintendent of the Chicago Police Department; Mitchell Ware, deputy superintendent of the department; Eugene Dorneker, a police department investigator assigned to the security section of the intelligence division; Mrs. Adelle Noren, a Chicago housewife who had served without remuneration as an informant within the Alliance to End Repression; and David Cushing, who had served as an undercover police officer in the Alliance to End Repression for over 5 years until his cover was blown.

Among other things, they testified that, pursuant to a legal action brought against the police department by the Alliance to End Repression and other organizations, the files of the intelligence unit had been sealed and placed under guard, so that the intelligence unit had had no access to them since March 26, 1975; and that the activities of the Alliance had effectively blown the cover of all Chicago undercover police officers and created a situation which makes it impossible for the Chicago Police Department to place any officer in undercover work. They warned that a continuation of the situation would make it extremely difficult for the department to take preventive action in dealing with extremist or terrorist activities and plans for violent demonstrations like "The Days of Rage" in November 1969.

In his prepared statement presented to the subcommittee, Superintendent Rochford made the following points:

Our total intelligence effort has been and will continue to be directed at the prevention aspect of violence, rather than at the enforcement aspect. Investigations of the Security Unit are targeted at: 1. Militant revolutionist and terrorist organizations; 2. Disruptive demonstrations requiring police manpower to exercise both crowd and traffic control; 3. Acts and threats of violence or disruption directed at people and at buildings; 4. Groups who have demonstrated a history of disruptive acts who function on the periphery of disorder by creating pressure situations.

Eugene Dorneker, who had been in charge of the investigation of the Alliance to End Repression for the Chicago Police Department, stated flatly that he considered the Alliance to be a Communist-front operation. He qualified this charge by noting that many of the organizations and individuals involved with the Alliance to End Repression were civic-minded and were neither Communist nor pro-Communist. He testified, however, that identified Communists had played a central role in the creation of the Alliance to End Repression and that they continue to play a key role in its current

operations. In support of this contention, he made the following points:

1. The Alliance to End Repression was founded through the efforts of the National Committee Against Repressive Legislation, which, in turn, resulted from the renaming of the National Committee to Abolish the House Un-American Activities Committee. Both of these organizations had been cited as Communist-front operations.

2. Richard Criley, who had played a central role in the founding of the Alliance, and who was currently serving as the executive director of the Chicago Committee to Defend the Bill of Rights, which works with the Alliance, had been identified by numerous persons in sworn testimony as a member of the Communist Party, and repeatedly invoked the fifth amendment when questioned by congressional committees about his Communist activities.

3. Jesse Prosten, a staff member of the Alliance to End Repression, has also been identified in sworn testimony as a member of the Communist Party.

Dorneker said that the Alliance sought to abolish all police intelligence, to discredit the police department in every possible way, to cultivate hostility against the police department in the public mind, and to establish "community" control over the activities of the police department. He said that the Alliance to End Repression had set up a police surveillance task force for the purpose of maintaining surveillance of officers assigned to the security unit, identifying informants, and bringing law suits, with a view to ultimately compelling the disbandment of the security unit.

Dorneker presented for the record an AER bulletin which claimed that Richard Gutman, a volunteer attorney working with the AER, had been able to identify police undercover agents in the AER by obtaining a copy of the Chicago Police Department's payroll roster, which contained, in addition to the names of the officers, their home addresses, and phone numbers. Dorneker said that he believed that Richard Gutman was the same Richard Gutman who, according to the records of the subcommittee, traveled to Cuba as a member of the Third Venceremos Brigade—ostensibly for the purpose of participating in the sugar cane harvest.

The AER bulletin reported that Gutman had subsequently met with Larry Green and Rob Warden, reporters for the Chicago Daily News, and had turned over this information to them. Subsequently, said Dorneker, he received a call from Warden, who told him that he knew that Adelle Noren and Dave Cushing were Chicago police agents. When he asked Warden how he had obtained his address and home phone number, Warden, he said, replied, "Because I happen to have a police department payroll computer readout of the whole thing by departments, which gives home addresses, telephone numbers."

The witnesses stated that, as a result of the revelations of the AER and the Chicago Daily News, one police undercover agent had been physically assaulted and several had received threatening phone calls.

Dorneker further stated that a large part of the funding for the Alliance to End Repression was supplied by the Law Enforcement Assistance Administration, a U.S. agency. Federal funds were given to the AER through a regional LEAA group called the Illinois Law Enforcement Commission. Federal funds were further disbursed

through a group under ILEC known as the Chicago-Cook County Criminal Justice Commission. The LEAA grants did not go directly to the AER, but indirectly through the Cook County Special Bail Project, an operation of the AER. The point was made that this was tantamount to supporting AER because of the sharing of facilities and personnel.

The Chicago-Cook County Criminal Justice Commission had on occasion rejected funding of the Alliance to End Repression group, only to have the AER approach the ILEC directly in order to overrule that decision.

Mr. Dorneker also stated that there were members of the ILEC who held office in, or were still connected, with the Alliance to End Repression. This fact gave the Alliance a very strong voice in receiving funds.

Dorneker said that—

Among those persons who have been appointed to the Illinois Law Enforcement Commission (ILEC) the following have been associated with the Alliance to End Repression:

Warren Wolfson, listed as a member of Board of Directors of the Alliance to End Repression's Cook County Special Bail Project, July 24, 1970. Withdrew as a member of Board July 1973, as he was appointed to the Illinois Law Enforcement Commission so as not to create a conflict of interest. Held meetings in his office with Cook County Special Bail Project members to advise them as late as January 1975.

James Taylor. June 1972, Taylor was a member of the Board of the Alliance to End Repression's Citizens Alert, and also a member of the Advisory Board of the Alliance's Cook County Special Bail Project.

Sgt. Arthur Lindsay. John Hill [a leader of AER] stated that when the Alliance to End Repression's project would not be funded, Sgt. Lindsay contacted him and said not to worry, that the project would be funded.

James Haddad. During meetings with Cook County States Attorney Carey, the Alliance to End Repression inquired as to who in his office the Alliance could establish as a contact. James Haddad was the contact between the Alliance to End Repression and the States' Attorney's office.

Mrs. Adelle Noren quoted Rev. William Baird, one of the founders of the AER, as saying: "We won't do anything unless we work with the Gus Halls." She presented for the record a copy of a flyer publicizing a rally and march sponsored by the AER and other organizations—including the Communist Party, U.S.A., the Socialist Workers Party (Trotskyites), and the Young Socialist Alliance (Young Trotskyites). The flyer was headed, "End Police Spying and Police Harassment, Abolish the Red Squad". She quoted Richard Criley as saying to her, "Each thing you do is a battle in the war, and therefore the battle must be handled in such a way that you win the war".

David Cushing, a police officer who served undercover in the AER, underscored the importance of coordinated intelligence in dealing with demonstrations that have a potential for civil disturbance. Com-

menting on the points made by Cushing, J. G. Sourwine, former chief counsel for the subcommittee, said:

As long as we are going to have terrorism and active demonstrations, whether they are violent demonstrations or planned as violent demonstrations, we are going to have blood in the streets and crossing State lines—we are going to have to have some method of coordinating intelligence. If you kill coordination through the elimination of all coordinating bodies, you've got nothing. If you eliminate police intelligence activities in major cities around the country, you've got nothing to start with.

The suit against the Chicago Police Department has not yet been resolved. But it is no exaggeration to say that the Alliance to End Repression and its allies, the American Civil Liberties Union and the National Lawyers Guild and the Communist Party, U.S.A., and the Trotskyists are already in a position to claim total victory.

- The files of the Chicago Police Department remain impounded.

- The intelligence unit, which in its better days had a complement of some 25 officers, has now been reduced to a meaningless custodial level of two or three men.

- The names of all police informants and undercover agents have been made public—either in consequence of revelations based on illegal access to police records or in consequence of court decisions. This has resulted in a situation where not even the most courageous and public-spirited citizen will in the future be willing to take the risk of serving as an informant for the Chicago Police Department or providing it with important information that may come to his attention.

- In consequence of all this, the current intelligence capability of the Chicago Police Department is zero.

Mr. Frank Carrington, Executive Director of Americans for Effective Law Enforcement testified that, whereas Chicago had remained relatively free of terrorist bombing incidents in the 1960's and early 1970's when the Police Department possessed an effective intelligence unit, there were two waves of serious terrorist bombings in 1975 and a number of other bombings in the period prior to his testimony. He said that no one had yet been killed but that was not the fault of the bombers. He mentioned the case of a bomb which had been placed in a wastepaper basket outside the Chicago Police Department's central headquarters. Fortunately, the bomb was spotted by an alert patrolman. Commenting on its potential for deadliness, Mr. Carrington said:

If it had exploded in that wastebasket—it was placed right where people come out of the subway entrance, and they are always in and out of the Chicago Police Department headquarters—then there could have been any number of people killed.

Mr. Carrington noted that the lawsuit by the Alliance to End Repression "has just put the intelligence function effectively out of business".

III. THE EXTENT OF THE EROSION

It is difficult to quantify precisely the extent of the erosion that has taken place in the field of law enforcement intelligence and the total impact of this erosion on American society. But from the totality of the testimony presented to the subcommittee, it is clear (1) that the scale of the erosion is already of a catastrophic order and (2) that the public and the Nation are paying a very high price in terms of reduced personal and corporate and national security, and escalating economic costs.

- Intelligence files laboriously built up over decades have in many cases been completely destroyed—i.e., State of Texas Public Safety Division; city of Baltimore; city of Pittsburgh; and Washington, D.C.

- In other instances, most notably the New York State Police and the Chicago Police Department, the intelligence files have been impounded now for several years—which, from a practical standpoint, has had the same impact as the physical destruction of the records.

- In many more instances—the New York Police Department and the Los Angeles Police Department are outstanding examples—there has been a massive purge of the files resulting in the elimination of 90 to 98 percent of the information on record.

- Intelligence units at State and local levels have been disbanded or reduced to so nominal a strength that they must be considered inoperative.

- The gathering of new intelligence—bearing on extremist activity as well as the activities of ordinary criminals—has become far more difficult because law enforcement agencies must now operate under the most severe restrictions governing the use of three of the most effective sources of intelligence: electronic surveillance, undercover agents and informants, and third-party records.

- Electronic surveillance in many jurisdictions has become a thing of the past, even where crimes like kidnaping and drug trafficking are involved. The subcommittee was informed that 21 States now prohibit wiretapping under any circumstances, while the laws of most other States restrict its use, even with court approval, to very rare instances.

- Third party records—bank records, phone and utility records, credit records, etc.—can only be obtained pursuant to court orders, and in many cases the regulations require that the subject involved be notified of the subpoena and given an opportunity to oppose its implementation. At the very least, this serves to alert the suspect that he is under investigation; at the worst, it makes it impossible for law enforcement to move rapidly enough to close in on criminal elements, who are always highly mobile.

- Law enforcement has suffered its greatest loss, however, in consequence of the dramatic reduction in the number of informants providing it with information. Informants now do not come forward as they used to do, for the simple reason that they fear disclosure of their identities under the Federal or State Freedom of Information Acts.

According to recent testimony before the House Intelligence Committee, the FBI, as of July 1978, was down to a total of 42 informants nationwide covering the entire field of terrorist and extremist groups.

Compounding all of these difficulties, there has been a virtual cessation in the sharing of intelligence by Federal, State, and local enforcement agencies. In the old days, intelligence on file with one law enforcement agency was available to other law enforcement agencies on a routine basis—in those days, there was no challenge to the commonsense proposition that, in dealing with organized crime or terrorism or foreign-sponsored activities, there was an imperative need to pool all of the available information. Witness after witness appearing before the subcommittee made the point that, as a result of the Freedom of Information Act and the Privacy Act, as well as the pervasive uncertainty and fear about what information may be released under State and Federal laws, the exchanging or sharing of law enforcement intelligence has been drastically reduced.

Several of the witnesses ventured estimates of the percentage fall-off in intelligence suffered by various law enforcement agencies.

- Mr. Glen King, executive director of the International Association of Chiefs of Police, estimated that the 17,000 municipal law enforcement agencies in the United States had in recent years lost between 50 and 75 percent of their total intelligence-gathering capabilities.

- Mr. Robert Chasen, the U.S. Commissioner of Customs, ventured the estimate that his agency had lost 40 percent plus of its intelligence capability. He said that one Regional Director of Investigations placed the estimate as high as 60 percent.

- Captain Dintino of the New Jersey State Police thought that his own intelligence unit may have lost as much as 50 percent of its effectiveness over a 2-year period.

The Secret Service does not gather intelligence information on its own. It operates on the basis of shared intelligence—that is by bringing together the totality of the intelligence available from Federal, State, and local sources—for the purpose of planning the protection of the President and the Vice President, the members of the Supreme Court, and foreign dignitaries. Because of the nature of its mission, there was no question in the minds of Mr. Knight and the other witnesses that it receives a greater degree of cooperation than any other law enforcement agency, including the FBI. However, Mr. Knight, in response to questioning, estimated that the Secret Service has suffered a falloff of 40 to 60 percent in the number of intelligence reports available to it on an annual basis, and that there was a further falloff of approximately 25 percent in the aggregate amount of intelligence available to the Service because the reports they were receiving were less detailed and comprehensive. What this added up to was that the Secret Service today was probably receiving only 25 percent of the amount of intelligence it used to receive before the era of privacy legislation.

These estimates do not, however, reflect the falloff in intelligence capabilities resulting from the attrition that has taken place in the field of sharing.

It is reasonable to believe that the falling-off in law enforcement intelligence nationwide, when proper allowance is made for the consequences of the near-freeze in the sharing of intelligence, is somewhat in excess of the estimates offered by Mr. Knight.

• The U.S. Capitol Police Force has the duty of protecting the Capitol and the Congress of the United States, at every level of law enforcement from simple criminal actions to the possibility of terrorism and mass disorders. To discharge its responsibilities, it relies heavily on the availability of intelligence from other law enforcement agencies. The importance of a free exchange of intelligence between law enforcement agencies was described in these terms by Chief Powell:

Prior to the enactment of the Freedom of Information Act, as amended, and the Privacy Act, law enforcement officers and agencies felt free to exchange information concerning persons or groups posing threats of potential violence or of massive disorder. We were able to plan and could therefore prepare for security with less show of force, as we felt that we had fair knowledge of what was being contemplated by the various groups, which we expected to be encountering on any given date.

All law enforcement professionals, and the distinguished members of this subcommittee, are thoroughly aware that in law enforcement we are wholly dependent for our effectiveness on rapid, timely, and reliable information from a wide range of sources, including: other law enforcement agencies; a concerned and cooperative public; non-law enforcement agencies of government; banks; businesses; schools; and others.

Our ability—collectively and cooperatively within the law enforcement community at all levels—to rapidly gather, assemble, analyze, retrieve, and disseminate among professionals in law enforcement information about crime and criminals is absolutely crucial to our role in providing a reasonably safe and wholesome environment for our citizens.

I am attempting to describe an open and straightforward system of collecting and evaluating data about criminals, criminal events, criminal conspiracies, or other activities that are apparently crime conducive. The collection and evaluation of such specific kinds of facts and details yields criminal intelligence—I prefer to say “criminal information” to avoid confusion with the past—that has a reasonable chance of leading to the identification of offenders and their successful prosecution.

Captain Justin Dintino, head of Criminal Intelligence for the New Jersey State Police, summed up the damage done by the restrictions on the exchange of intelligence in the following terms:

The free flow of intelligence between Federal, State, and local agencies is essential to an effective law enforcement operation. To the extent that this flow is restricted, law enforcement is handicapped. And today this flow is terribly restricted, at every level and in every direction: From city to city, from State to State, from State agencies to Federal agencies, and from Federal agencies to the State and local level. This is a disastrous situation and we've got to find some way of reversing it.

IV. THE CONSEQUENCES OF THE EROSION: A GENERAL SUMMARY

The erosion of law enforcement intelligence and the complex of circumstances contributing to this erosion or resulting from it, have affected the security of the American people and American security at every level.

The security of the citizen is directly and seriously affected by existing privacy legislation. Background checks, per se, are not directly prohibited by law. But, as will be discussed later, a combination of constraints has made effective background checks virtually impossible.

This has placed every individual in greater jeopardy from criminal elements because, under the restrictions that exist today, hospitals cannot do background checks on their employees to make certain that they are not hiring convicted rapists or arsonists, nor can such background checks be performed on telephone and utility repairmen and other employees whose position gives them access to private homes.

It has seriously affected corporate security for the simple reason that a bank cannot check to find out if an applicant for a position as an accountant is a convicted embezzler; a research laboratory or an engineering firm cannot check to find out if an applicant has a record of technology theft; a truck company cannot check to find out if a driver it is about to hire has been involved in hijackings; and the company in charge of the construction of the Trans-Alaska Pipeline, as previous testimony before the subcommittee confirmed, was unable to do background checks on its labor force to make sure that it was screening out terrorist and other extremist elements, as well as ordinary psychopaths.

The erosion of law enforcement intelligence has adversely affected the security of society by reducing and in some cases nullifying law enforcement restraints directed against organized crime.

It has weakened internal security by drastically limiting or even eliminating intelligence relating to subversive and extremist organizations. Under the generally prevailing guidelines today, law enforcement agencies are not permitted to make any intelligence entry based on what is euphemistically called "mere membership"—whether the membership involves the Communist Party, U.S.A., or the Trotskyists, or the Puerto Rican Socialist Party, or the American Nazi Party, or the KKK, or any of the other organizations of the extreme left or the extreme right. In order to make an intelligence entry, there must be some overt act resulting in an indictment or conviction.

Nor are our law enforcement authorities, under existing restrictions, able to protect society effectively against organized terrorist groups. The subcommittee, in October 1975, took testimony from the officers in charge of the bomb squads in New York, Los Angeles, San Francisco, and Dade County, Fla. All of them complained that the absence of intelligence and the restrictions that were placed on them made it

impossible for them to protect their communities by anticipating bombing and moving to prevent them. As one of them put it, they were always in the position of "playing catchup ball," of reacting to bombings after they had taken place.

The Hanafi Muslim siege in Washington, D.C., in the spring of 1976 is, perhaps, one of the most dramatic examples of the damage that can be done by the destruction of intelligence capabilities. In the 1960's and early 1970's, the District of Columbia Metropolitan Police Department, like every other major police department, maintained an intelligence unit and intelligence files, and used the traditional instruments of surveillance and informants to keep track of activities that might imperil the community. But then, as a result of pressures from the District of Columbia City Council, the intelligence unit was disbanded; all intelligence files were destroyed, including the file on the Hanafi Muslims; and all informants were called off, including, again, an informant in the Hanafi Muslims. Had the District of Columbia Police been receiving reports on a regular basis from an informant who had infiltrated the Hanafi ranks, the chances are 100 to 1 that they would have had intelligence enabling them to take preventive action. Having been reduced to a zero intelligence capability, the District of Columbia Police were in no position to take preventive action against anything. The consequence was that the Hanafi Muslims, with no opposition, were able to take over the District Building, the B'nai B'rith Building, and the Moslem Mosque and Cultural Center. One man was killed, another crippled for life, and several hundred hostages suffered a traumatic experience that left them psychologically scarred for years to come.

The Secret Service is charged with the responsibility of protecting the President and other V.I.P.'s—domestic and foreign. But even the security of the President and of the Secret Service's other protectees has been imperiled by the erosion of law enforcement intelligence. As was pointed out in the previous section, Mr. Knight, Director of the Secret Service, told the subcommittee that the Secret Service was now receiving probably only 40 percent of the information it used to receive and that the erosion in the quality of this intelligence may have reduced the effectiveness of their overall intelligence input by a factor of perhaps another 25 percent. When he was asked what the Secret Service does when the President is planning to visit a city like Chicago, where the files have been locked up for several years and the intelligence unit has been reduced to a residual operation, Mr. Knight replied that there were situations where the Service had to rely on what he called "institutional memory," and attempt to compensate for the deficiencies in its intelligence by pumping in more manpower. The first procedure he considered risky; the second procedure is very costly and obviously places a heavy strain on manpower resources. When Mr. Knight was further asked whether there were any cities where the situation was so bad that they had advised the President, or would advise the President, not to visit, he replied that there were such cities, but that he preferred not to name them in public session.

The same restrictions and the same philosophy that have done so much damage to law enforcement intelligence at the Federal, State, and local levels, have also been responsible for the virtual dismantling of the Federal Employee Security Program. On the one hand, the Civil Service Commission no longer gets the willing cooperation of

law enforcement agencies around the country in doing background checks on applicants for Government employment; and schools and neighbors and other sources are far more reluctant to provide information than they used to be. On the other hand, the Civil Service Commission has progressively trimmed its own criteria to conform with the spirit of the times, so that today no one can be denied employment, even in a sensitive position, on the basis of "mere membership" in the Communist Party, U.S.A., or the American Nazi Party or other organizations of the extreme left or right; denial of employment has to be based on an overt violation of the law.

Commenting on this situation, Senator James O. Eastland, chairman of the Senate Judiciary Committee, and Senator Strom Thurmond, ranking minority member, said in a joint letter on March 1, 1978 to Alan K. Campbell, Chairman of the U.S. Civil Service Commission:

We find it difficult to avoid the conclusion that, over the past 5 years or so, without the knowledge of Congress, and contrary to statutory requirement and the Commission's own regulations, there has been a progressive dismantling of the Federal Loyalty-Security Program—until today, for all practical purposes, we do not have a Federal Loyalty-Security Program worthy of the name.

The weakening of the general fabric of law enforcement has resulted in a tremendous increase in the field of private security and security hardware. Indeed, as one witness told the subcommittee, the business of security may now be the Nation's No. 1 growth industry—the membership of the American Society for Industrial Security, it was pointed out, had virtually doubled in a few years' time. When the panel of private security experts was asked whether it was not possible that, as a result of our excessive concern for privacy, we were in the process of converting our country into a "garrison state", one of the witnesses replied that, in his opinion, "we already are a garrison state".

The pyramiding costs of private security and the pyramiding losses suffered by banks and insurance companies and stores and hospitals and other private corporations, are, needless to say, reflected in the sharply increased costs which every consumer must today pay for insurance and medical care and for virtually everything he purchases.

Over and over again, the subcommittee was told by witnesses from the law enforcement community that the only elements in our society who had really benefited from the erosion of law enforcement intelligence were the criminal community and the political extremists. As Laurence Silberman, former Deputy Attorney General, told the subcommittee:

... I cannot help but believe that anything which improperly diminishes the effectiveness of law enforcement capabilities by striking at the possibility of generating legitimate law enforcement intelligence must aid those forces, both domestically and in foreign intelligence, whose purposes are deleterious to the United States.

V. IS LAW ENFORCEMENT INTELLIGENCE LEGAL? A SUMMARY OF COURT RULINGS

The question whether law enforcement intelligence is legal may at first glance appear to be an extreme formulation, but it is not extreme when viewed in the context of the voluminous testimony taken by the subcommittee.

Mr. Frank Carrington, executive director of Americans for Effective Law Enforcement, told the subcommittee that—

Since the night that five men broke into the Watergate complex to gain information for the partisan political purposes of their principals, the terms "intelligence gathering" and "national security" have become dirty words. The news media and those organizations for whom individual privacy is an end in itself have parlayed the outrages of Watergate into a concerted effort to dismantle the intelligence gathering apparatus of law enforcement agencies. Hardly a day goes by that we do not hear of some new accusation of "illegal" police "spying." Thus, the question whether or not intelligence gathering activities are inherently illicit takes on an enormous significance.

In response to this question, Mr. Carrington and Charles E. Rice, professor of law, University of Notre Dame, summarized a whole series of decisions by the Supreme Court of the United States and other Federal courts and by State supreme courts upholding the legality of law enforcement intelligence activities, in response to suits which sought to have them declared illegal or unconstitutional.

Mr. Carrington noted that—

A great deal of current criticism of the police intelligence function is directed against the police practices of being present at events, meetings, or gatherings of so-called political or dissident groups. This may be done overtly by law enforcement officers in uniform or by those in plain clothes who make no effort to conceal the official nature of their presence. It may be done covertly by undercover policemen or police informants who attend the event without making their presence known. These practices have been challenged in lawsuits that allege that the presence of law enforcement officers, either overt or covert, somehow "chills" the participants' rights of freedom of assembly and expression.

Among the cases quoted by Messrs. Rice and Carrington was the decision in *Anderson v. Sills*, handed down by the New Jersey Supreme Court in June 1970. This suit was an outcome of the massively destructive riot in the city of Newark which took place on June 1, 1967. Reacting to this riot, the Governor of New Jersey conferred with the mayors of the cities of New Jersey to consider what measures could be taken to prevent similar outbreaks from recurring.

The conference produced a memorandum from the State Attorney General to local law enforcement units, in effect asking for their cooperation with the State in preventing or controlling such public disorders, by sharing intelligence.

The Jersey City branch of the NAACP and the SDS group at St. Peters College in Jersey City at this juncture filed a class action suit against the State Attorney General, the Jersey City police chief, and others, claiming that the plan to gather and share intelligence violated their first amendment rights, and they asked for injunctive relief. The trial court of the first instance granted a summary judgment, but this judgment was unanimously reversed by the State Supreme Court. Writing for the court as a whole, Chief Justice Weintraub said, in this historic decision:

Here we are dealing with the critical power of government to gather intelligence to enable it to satisfy the very reason for its being—to protect the individual in his person and things. The question in this case is not merely whether there are some individuals who might be “chilled” in their speech or associations by reason of the police activity here involved. Rather the critical question is whether that activity is legal, and although the amount of “chill” might in a given case be relevant to the issue of legality, the fact of “chill” is not itself pivotal. Indeed, the very existence of this Court may “chill” some who would speak or act more freely if there were not accounting before us for trespasses against others. But government there must be, for without it no value could be worth very much. The first amendment itself would be meaningless if there were no constitutional authority to protect the individual from suppression by others who disapprove of him or the company he keeps. Hence the first amendment rights must be weighed against the competing interests of the citizen. If there is no intent to control the content of speech, an overriding public need may be met, even though the measure adopted to that end operates incidentally to limit the unfettered exercise of the first amendment right.

* * * * *

The police function is pervasive. It is not limited to the detection of past criminal events. Of at least equal importance is the responsibility to prevent crime. In the current scene, the preventive role requires an awareness of group tensions and preparations to head off disasters as well as to deal with them if they appear. To that end the police must know what forces exist; what groups or organizations could be enmeshed in public disorders. This is not to ask the police to decide which are “good” and which are “bad.” In terms of civil disorders, their respective virtues are irrelevant, for a group is of equal concern to the police whether it is potentially the victim or the aggressor. The police interest is in the explosive possibilities and not the merits of the colliding philosophies. And it must be evident that a riot or the threat of one may best be ended with the aid of private citizens who because of their connections with the discordant

groups can dissuade them from a course of violence. Hence a police force would fail in its obligation if it did not know who could be called upon to help put out the burning fuse or the fire.

On the specific question of the use of informants for intelligence gathering purposes, Mr. Carrington quoted a 1971 decision of a Federal court in *Bagley v. City of Los Angeles Police Department*. This decision was in response to a Federal civil rights suit which sought to ban the attendance of police undercover agents at college classes. The court ruled:

(The) use of undercover agents for the purpose of obtaining evidence relating to past, present or future criminal activity is an approved police technique, even though its effectiveness often depends upon deception and secrecy. The admissibility of such evidence in a subsequent proceeding is another question with which we need not be concerned here. The use by police of deception and secrecy in this context is not impermissible and the fact that the innocent as well as the guilty may also be deceived is not in itself significant.

* * * * *

The constitutional intrusion of which the plaintiffs complain, is that of an invasion of their right of privacy. But we know of no rule or law, constitutional or otherwise, which gives a student in a classroom the right to restrict the use of statements made by him in open discussion or which protects him from the consequences of what he says or does.

Mr. Carrington also referred to the decision in *Socialist Workers Party v. Attorney General* handed down in December 1974, by Supreme Court Justice Thurgood Marshall.

The Socialist Workers Party (SWP), an organization whose literature makes it clear that it considers itself Trotskyist Communist, had been under surveillance for many years and had been cited as subversive by the Attorney General in 1948. The SWP had filed suit asking the U.S. Southern District Court in New York to enjoin the FBI from surveilling the planned convention of its youth organization, the Young Socialist Alliance, in St. Louis, Mo., at the end of December 1974. In this suit, the SWP charged that the presence of FBI informants and infiltrators at the convention would "chill" their first amendment rights of freedom of speech and assembly. The requested injunction was granted by the district court. However, when the Attorney General appealed this decision, the Second Circuit Court of Appeals overturned the decision of Judge Griesa, criticizing him for his "rush to judgment" and "abuse of discretion".

The SWP appealed the ruling of the Second Circuit Court of Appeals to Supreme Court Justice Marshall. Justice Marshall rejected their appeal. They then carried their appeal to Justice Lewis F. Powell, Jr., who also turned them down.

Justice Marshall, in his decision, wrote:

It is true that governmental surveillance and infiltration cannot in any context be taken lightly. But our abhorrence for abuse of governmental investigative authority cannot be

permitted to lead to an indiscriminate willingness to enjoin undercover investigation of any nature, whenever a countervailing first amendment claim is raised.

In this case, the court of appeals has analyzed the competing interests at some length, and its analysis seems to me to compel denial of relief. As the court pointed out, the nature of the proposed monitoring is limited, the conduct is entirely legal, and if relief were granted, the potential injury to the FBI's continuing investigative efforts would be apparent. Moreover, as to the threat of disclosure of names to the Civil Service Commission, the court of appeals has already granted interim relief. On these facts, I am reluctant to upset the judgment of the court of appeals.

The U.S. Court of Appeals decision in *Socialist Workers Party v. Attorney General*, which Supreme Court Justice Thurgood Marshall upheld, was noteworthy for its comprehensive review of legal precedents having a bearing on the case and for its frank consideration of the SWP's ties with the Fourth International and the involvement of elements of the Fourth International in terrorist activities.

In ruling against the SWP, the Court of Appeals quoted from a 1972 Supreme Court decision on wiretapping (*United States v. District Court*, 407 U.S. 297):

Unless Government safeguards its own capacity to function and to preserve the security of its people, society itself could become so disordered that all rights and liberties would be endangered.

It is also quoted Chief Justice Holmes of the Supreme Court as saying in *Cox v. New Hampshire*:

Civil liberties, as guaranteed by the Constitution, imply the existence of an organized society maintaining public order, without which liberty itself would be lost in the excesses of unrestrained abuses.

Expanding on this, the decision of the Court of Appeals stated:

The FBI has a right, indeed a duty, to keep itself informed with respect to the possible commission of crimes; it is not obliged to wear blinders until it may be too late for prevention.

The Court of Appeals decision went on to quote from the ruling of Judge Weinfeld, district court judge in New York City (*Handschu v. Special Services Division*, October 24, 1972):

The use of informers and infiltrators by itself does not give rise to any claim of violation of constitutional rights.

Finally, the Court of Appeals decision quoted the historic words of Supreme Court Justice Jackson in *American Communications Association v. Douds* (339 U.S. 332):

The Court's day-to-day task is to reject as false, claims in the name of civil liberty which, if granted, would paralyze or impair authority to defend the existence of our society, and to reject as false, claims in the name of security that would undermine our freedoms and open the way to oppression.

Also quoted by Messrs. Carrington and Rice was the decision of the New York Second Court of Appeals in *Fifth Avenue Peace Parade Committee v. L. Patrick Gray* (480 F. 2d 326), June 12, 1973. This decision came in response to a class action suit against the FBI charging that its investigation of the organization's participation in the mass demonstration against the Vietnam War in Washington, D.C., in November 1969, involved an invasion of their constitutional right of privacy; that it had a "chilling" effect on their first amendment rights; and that it constituted unlawful search and seizure. The Fifth Avenue Peace Parade Committee asked the court that the information gathered by the FBI be surrendered or destroyed, and that it never be used in any way.

In justifying the FBI's surveillance activities against the Fifth Avenue Peace Parade Committee, an FBI witness told the court that the purpose of this surveillance was:

To know who was coming, how many were coming, mode of transportation, arrival, when they expected to leave Washington, any individuals that had a potential record of violence, or who might threaten the President's life, or a Cabinet member, or anything of that nature.

The Court of Appeals, in rejecting the suit of the Fifth Avenue Peace Parade Committee, stated:

Beyond any reasonable doubt, the FBI had a legitimate interest in and responsibility for the maintenance of public safety and order during the gigantic demonstration planned for Washington, D.C. In fact, had it been ignored the agency would be properly chargeable with neglect of duty . . . the assemblage of the vast throng . . . presented an obvious potential for violence and the reaction of the Government was entirely justifiable.

On the question of third-party records, Mr. Carrington, while noting that some courts have taken a more restrictive attitude toward the inspection of such records by law enforcement officers, nevertheless pointed out that there existed a whole series of legal decisions upholding the propriety of such investigative procedures. He noted, among other things, that "in 1976, the Supreme Court held that fourth amendment rights were not violated when law enforcement officers examined third-party records without a warrant." *U.S. v. Miller*, 44 USLW, 4528, 421/76).

Examining a series of decisions dealing with the dissemination of information among law enforcement agencies, Mr. Carrington testified that, while a showing of innocence and a few other circumstances provided some exceptions to the rule, "the basic rule is that law enforcement may collect, retain, and exchange with other law enforcement agencies information relating to criminal justice and intelligence. In fact, a line of cases permits the exchange of such information."

In the fall of 1971, the American Civil Liberties Union launched its "Political Surveillance Project." This project was described in the following terms in the ACLU's 1970-71 report:

The ACLU has made the dissolution of the Nation's vast surveillance network a top priority . . . The ACLU's attack

on political surveillance is being pressed simultaneously through a research project, litigation, and legislative action.

Apart from the ACLU and a handful of more radical organizations like the National Lawyers' Guild and the Alliance to End Repression, there are no significant national organizations that have argued for the complete abolition of the political surveillance activities that have been—and on a much reduced scale, still are—targeted against extremist political groups of both the far Left and the far Right. Not even the ACLU and the Guild have championed the total elimination of intelligence programs targeted against simple criminal activities such as drug trafficking and conspiracy to commit larceny or kidnaping or arson. But 7 years after the ACLU announced the launching of its campaign to completely eradicate all surveillance of political groups—no matter how radical or how committed to violence—the ACLU can now boast that it is within measurable distance of complete success. As for ordinary criminal intelligence, the restrictions that have been imposed at State, Federal, and local levels over the past decade and the massive destruction of files and records and the damaging effects of the Freedom of Information and Privacy Acts have created a situation surpassing the dangers that even the most concerned observers foresaw.

VI. FACTORS CONTRIBUTING TO THE EROSION (II): THE FREEDOM OF INFORMATION ACT AND THE PRIVACY ACT

The central role played by the Freedom of Information Act and Privacy Act of 1974 in undermining the capabilities of law enforcement intelligence was stressed in the testimony of numerous witnesses. Before summarizing the massive testimony dealing with the damage done to law enforcement at every level in consequence of these two measures, it might be useful to briefly review their philosophical and political background and legislative history.

THE FREEDOM OF INFORMATION ACT

The Freedom of Information Act is based on the presumption that all Government information should be available to the public unless there are compelling reasons relating to national security or law enforcement or privacy which justify exemption. This presumption, in turn, is based on the hallowed conviction, implicit in the Constitution, that citizens have a right to know what their Government is doing, so that they can intelligently pass judgment on its actions, and so that Government may truly derive "its just powers from the consent of the governed."

Even before the Vietnam War—in part as a result of investigations conducted by the House Government Operations Special Subcommittee on Government Information under the chairmanship of Representative John E. Moss—there was a growing conviction that Government was being too secretive about too many things. It is only natural that secretiveness, or a perception of secretiveness, should inspire distrust; the assumption is that the secretiveness is being used to cover up a host of crimes and improper activities by those agencies and persons who invoke its protection. This assumption was greatly fortified in the late 1960's and early 1970's by the Watergate crisis and a series of prior and subsequent revelations of criminal or improper activities by members of the executive branch, by Congressmen, and by prominent members of the judiciary.

It was against this background that Congress, in 1966, enacted the first Freedom of Information Act. In signing this act on July 4, 1966, the late President Johnson summed up its motivation and its intent in these words:

This legislation springs from one of our most essential principles: A democracy works best when the people have all the information that the security of the Nation permits. No one should be able to pull curtains of secrecy around decisions which can be revealed without injury to the public interest.

Through the late 1960's, inspired by the growing fear of computerized data collection and dissemination, there were numerous studies and hearings having to do with the general subject of Federal and corporate recordkeeping and personal privacy. Congressional sub-

committees looked into such matters as the automation of Government files, Justice Department data collection activities, the Census Questionnaire, the personal data operations of credit agencies, the confidentiality of student records, and the use of polygraphs. These hearings and studies resulted in the inclusion of stringent privacy provisions in the Fair Credit Reporting Act of 1970, the Crime Control Act of 1973, the Family Educational and Privacy Act of 1974, and finally—and most significantly—in the amended Freedom of Information Act of 1974.

The amended FOIA, which was far more sweeping in its disclosure requirements than the original FOIA, was a product of the conviction on the part of Congress that the FOIA of 1966 was not achieving its objectives. A House subcommittee report in 1972 charged that "the efficient operation of the Freedom of Information Act has been hindered by 5 years of foot-dragging by the Federal bureaucracy . . . in parts of two administrations." Among other things, it was charged that the prime beneficiaries of the statute were not the public or the media but big business. It was alleged that this was so because the utilization of the act required a combination of money and legal expertise and time which the average citizen could not afford.

One of the major changes in FOIA of 1974 reduced the ability of Government agencies to exempt investigatory records from disclosure. There was no longer to be any blanket exemption of investigatory files; only files having to do with active investigations could be withheld. Otherwise, each document in the file, each page, and each paragraph in each document had to be carefully checked for the purpose of assuring the maximum possible disclosure.

The original FOIA required that documents requested under FOIA be "identifiable". It had been argued that this emphasis on identifying the documents requested could be used by agencies to give themselves an out. The revised act, therefore, said that a request under FOIA need only "reasonably describe" the material sought.

In addition, agencies were required to respond in 10 days to a request for information.

Exemptions were to be granted only where the production of the requested records would:

- (1) Interfere with enforcement proceedings; (2) deprive a person of the right to a fair trial; (3) constitute an unwarranted invasion of personal privacy; (4) disclose confidential sources or, in certain circumstances, information provided by such sources; (5) disclose investigative techniques and procedures; or (6) endanger law enforcement personnel.

Although FOIA had been passed by overwhelmingly large margins in both houses of Congress, President Ford vetoed the measure on October 17, 1974, justifying his veto on the grounds that it would adversely affect the retention of military and intelligence secrets, would compromise the confidentiality of investigatory law enforcement files, would unreasonably burden agencies in imposing specific response times, and was otherwise "unconstitutional and unworkable". The House voted to override President Ford's veto by 371 to 31 on November 20, 1974, and the Senate followed suit the next day by a vote of 65 to 27.

The sponsors of the FOIA wanted to reinforce the citizen's right to know; they wanted more open Government; they wanted to put an end to the abuses perpetrated in the name of Government secrecy and executive privilege. It can safely be said that none of them foresaw the host of difficulties the legislation would create for the law enforcement community, nor did they foresee the utilization that would be made of the act by organized crime and other criminal elements or the damage it would do to the personal security of the individual citizen. With the testimony on these points, we shall deal in detail after examining the history of the Privacy Act.

THE PRIVACY ACT

The point has been made that, unlike the "right to know" which FOIA sought to translate into legislative language, the right to privacy is not expressly written into the Constitution. The concept, rather, is the product of a series of writings and Supreme Court decisions in recent decades.¹

The first effort to define a right to privacy based on the Constitution has been attributed to Justice Brandeis' dissent in *Olmstead v. United States*, a case in which wiretaps had been used to obtain bootlegging evidence. Justice Brandeis wrote:

The makers of our Constitution . . . conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the fourth amendment.

Despite Justice Brandeis' eloquent dissent, the Supreme Court admitted the evidence in the *Olmstead* case. It has been noted, however, that Justice Brandeis' basic views in this case subsequently influenced a series of Supreme Court decisions, all of which had the effect of reinforcing the legal barriers to the invasion of privacy.

The 1950's and 1960's witnessed a growing concern over the problem of privacy, fed by the increasingly widespread use of polygraph testing and the publication of best selling books like "The Eavesdroppers" by Samuel Dash, and "The Naked Society" by Vance Packard.

Before the enactment of FOIA in 1974, there had already been a series of hearings, over a period of several years, dealing with the broad issue of privacy. On the heels of the Freedom of Information Act, and for the avowed purpose of reinforcing it, Congress, in November 1974, passed the Privacy Act. The vote once again was completely lopsided. In the Senate, the vote was 74 to 9. In the House it was 353 to 1.

The preamble to the Privacy Act of 1974 describes its purpose as follows:

The act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to—

¹Hanus, Jerome J. and Relyea, Harold C., "A Policy Assessment of the Privacy Act of 1974," the American University Law Review, vol. 25, No. 3, Spring 1976, p. 562.

permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies;

permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;

permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;

collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;

permit exemptions from the requirements with respect to records provided in this act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

be subject to civil suit for any damages which occur as a result of willful or intentional action that violates any individual's rights under this act.

Once again, the language of the act was noble, the motivations were beyond reproach—but the reality that has emerged from the legislation has in many important respects deviated sharply from the purposes intended by its framers.

THE PRACTICAL CONSEQUENCES OF FOIA/PRIVACY ACT

Witnesses before the subcommittee agreed on the point that the Freedom of Information Act had brought some genuine benefits.

Mr. Quinn Shea, of the Justice Department, enumerated the following benefits which he believed had redounded to the advantage of law enforcement from the privacy legislation.

He said that "releases under the act have definitely tended to assist in the restoration of public confidence in Government in general and criminal justice law enforcement in particular."

Next, he said, instead of acquiring and keeping data simply for the purpose of acquiring and keeping it, the component agencies of the Justice Department "have begun the desirable process of studying just what data they really need to acquire, how it should be used, and how long it should be retained."

He also said that the Justice Department feels that "access by inmates to most of the records in their prison files has operated to reduce tension in our confinement facilities."

Mr. Shea also argued that the statutes represented another plus for law enforcement in the sense that "they constitute specific, if imprecise, recognition by Congress that criminal justice records can be properly withheld under certain circumstances."

Mr. William Williams, Deputy Commissioner of the Internal Revenue Service, also felt that FOIA and the Privacy Act had resulted in some distinct benefits. He testified:

On balance, we believe that, to date, these acts have had a beneficial influence upon the tax administration process. Today, for example, all of the IRS administrative procedures and operational handbooks, with the exception of our law enforcement manual are available to the public upon request. Portions of the manual, are being published by one of the major tax services. Prior to FOI, these materials were kept confidential, although subsequent experience has demonstrated no legitimate tax administration function was served by this restriction.

With this access, individuals, the media, and public interest groups have done much to identify shortcomings in our procedures which the Service, in turn, has moved to correct—that is, it has improved publicity to all taxpayers regarding their appeal rights, and the streamlining of our appeals procedure.

Other witnesses from the law enforcement community were also agreed that FOIA and the Privacy Act had, in certain important respects, resulted in an improved situation. All of them were agreed on the general need for legislation in these areas.

Witness after witness, however, testified that FOIA and the Privacy Act, in their current form and as they are currently administered, have crippled law enforcement intelligence and hobbled law enforcement in general. Their attitude was perhaps best summed up in the words of Professor Charles Rice of Notre Dame—

It should not be supposed . . . that the FOIA and PA have not achieved good ends. They were enacted to meet a genuine need for more openness in government, on the one hand, and, on the other, more protection for the right to be left alone. What is necessary now is not a dismantling of those statutes but rather corrective surgery to bring them more into line with their original and laudable purpose.

The matter of costs

The cost of administering the Freedom of Information Act, in terms of both money and manpower, was a general subject of complaint.

Mr. Laurence Silberman, former Deputy Attorney General, testified that the actual costs of implementing the Freedom of Information Act far exceeded the original estimates. He said that the cost to the FBI alone for fiscal year 1977 was almost \$13 million, and that the work of processing FOIA/Privacy Act requests had taken 375 persons, including 50 highly trained agents, away from other activities. He added that it was his understanding that "200 extra agents had been called in on an emergency basis to try to deal with the backlog" in requests.

Commenting on the same situation, Mr. Quinlan J. Shea of the Justice Department told the subcommittee:

. . . it is a fact that right now something in excess of 6 percent of the FBI's total personnel complement is working in the area of the Freedom of Information and Privacy Acts, full time, plus other people who are not involved on a full time basis. That is a rather high percentage of the personnel resources of a law enforcement organization.

On July 18, 1977, Senator Eastland asked the General Accounting Office (GAO) to prepare an agency by agency breakdown of the costs of administering FOIA and the Privacy Act, including the costs of workloads of cases in litigation. GAO was further asked to determine how much these costs had increased on a year-to-year basis since the two acts became law, and to project the costs over the coming 5-year period.

In its June 16, 1978, response to this request, the GAO noted that both the Office of Management and Budget (OMB) and the Congressional Research Service (CRS) had conducted studies of FOIA/Privacy Act costs in 1976. OMB and CRS had both found that the accounting systems vary tremendously from agency to agency, making a precise cost estimate impossible. While noting that the CRS had questioned the meaningfulness of the FOIA cost data, the report stated that 35 agencies reported FOIA costs of \$11.8 million in the calendar year 1975, while 37 agencies reported costs of \$20.8 million for 1976. In the case of the 13 agencies for which GAO sought to obtain 3-year cost estimates, GAO reported that the total cost, including startup cost, for the period 1975-77, amounted to \$35.9 million.

The GAO summary of cost data for processing FOIA/Privacy Act requests in thirteen agencies is printed as an appendix to this report.

The money costs associated with the implementation of FOIA/Privacy Act are high but certainly not astronomical in terms of today's agency budgets. But the implementation of FOIA/Privacy Act has done far greater damage to the effectiveness of several of our major agencies than the dollar figures themselves suggest. Because of the difficulty of going through highly sensitive files and making judgments on a page-by-page, word-by-word basis, the FBI, the DEA, the IRS and other agencies have had to assign large numbers of their most experienced analysts and investigators to the thankless task of processing requests under FOIA and the Privacy Act. It is self-evident that other agency activities and the quality of law enforcement in general are bound to suffer when so many of the most qualified investigators and analysts are, for all practical purposes, removed from the field of law enforcement.

Mr. Williams of IRS said that the two acts had produced a heavy workload for his agency, requiring responses to 15,540 requests in 1975, and a smaller but nonetheless heavy workload of 7,913 requests in 1977. He made the point, however, that the apparent reduction in requests involved primarily a reduction in the number of requests for manual materials, but that "the number of requests for investigatory records has continued to grow". Said Mr. Williams:

Data for calendar year 1977 show that, of 23,347 hours contributed by professional employees in IRS field offices—other than our specialists in the FOI area—professionals

in the Intelligence Division provided 10,514 hours and professionals in the Audit Division provided 5,893 hours. We believe that these figures suggest a significant incident of use of the Freedom of Information Act by the subjects of IRS law enforcement activities to secure investigatory files concerning themselves.

While the diversion of staff resources to process Freedom of Information Act and Privacy Act requests clearly has a negative impact on our enforcement capabilities, this direct reduction does not represent the only effect of these statutes upon law enforcement. There are significant but intangible costs of processing FOI Act requests which cannot be captured statistically. For instance, when a request is made for an open investigatory file, the steps necessary to process that request will tend to disrupt the investigation and will generally require the temporary diversion of investigative staff.

The Drug Enforcement Administration made available to the subcommittee an internal memorandum dealing with FOIA's heavy demands on professional manpower. The memorandum said:

When the Freedom of Information Act was passed, no funds were appropriated to the Executive Branch to administer the Act. Therefore, all positions in the Freedom of Information Division were taken from ceilings allotted to other units or activities within DEA.

Some comparative figures on the commitment of resources to administer the Act, as opposed to the resources committed to accomplishing our primary mission are startling.

The fifteen employees assigned full time to the Freedom of Information Division represent fifty percent (50%) of our investigative commitment in the Republic of Mexico, twenty-nine percent (29%) in Europe, twenty-eight percent (28%) in South America, thirty-eight percent (38%) in Southeast Asia, sixty percent (60%) in the Near East, one hundred percent (100%) in the South Pacific, and two hundred-fourteen percent (214%) in Canada.

In addition, the Freedom of Information Division is larger than any of our six (6) Internal Security Field Offices, equals or is larger than the agent commitment of eighty (80) of our domestic District Offices, is larger than the individual sections within the Enforcement and International Training Divisions, and is larger than the resources committed to the various sections of the Office of Intelligence.

IRS stated to GAO that in many instances "the value of the resources withdrawn from the investigatory effort may be far more costly in terms of lost revenue opportunities than the direct cost ascribed to processing the FOIA requests".

A total assessment of the costs of FOIA and the Privacy Act would have to include all of the factors listed above.

WHO ARE THE REQUESTORS?

In taking the testimony of spokesmen for the various agencies involved in the hearings, the subcommittee sought to obtain a rough understanding of the categories of people who have been making the heaviest use of the privileges accorded them under FOIA and the Privacy Act. The questions sought a breakdown by the following categories: media, students, curious citizens, criminal elements, and extremists.

The general picture that emerges from this part of the investigation is that a breakdown of requestors will vary from agency to agency. In the case of certain agencies, there can be no doubt that the overwhelmingly majority of requests come from ordinary, law-abiding citizens, including curiosity seekers. A heavy volume of the requests submitted to the FBI and DEA, however, come from the criminal community and members of extremist organizations.

Mr. Bensinger of DEA told the subcommittee that 40 percent of the total number of requests received by his agency came from convicted felons, many of them serving time in prison. The DEA, he said, had been inundated with form letter FOIA/Privacy Act requests from prisoners and organized dissident groups in prison—in each case seeking to discover what DEA may know about their criminal activities. He said that in such cases it is obvious that a standard form letter is prepared by someone and then Xeroxed and passed around to other prisoners. He confirmed to the subcommittee that requestors do not confine themselves to a simple letter of request, but will harass the agency by writing 15, 20, or 30 or more different letters, requesting variations on the same information.

The following exchange took place on the subject of some of the highly sensitive information that has been released to convicted felons under FOIA:

Senator THURMOND. The subcommittee has heard of another case where a prison inmate, acting under the Freedom of Information Act, requested a copy of a Drug Enforcement Administration publication describing the procedures used by criminal elements to manufacture liquid hashish.

According to our information, this information was sent to him. Do you know about this case?

Mr. BROSAN. Yes, sir. That was information concerning the simplified methods of manufacturing liquid hashish, which was contained in an intelligence brief which we used for the training of our own personnel. We had several requests for the material. We denied those requests, but we were later overruled by the Department of Justice appeals unit.

In fact, we have disseminated that information.

Mr. SHORT. In the case of the prisoner, Department of Justice overruled your denial and the documents were sent. I believe, however, that when the documents reached the prison the warden refused to release them, because this was not the type of material that should be given to prisoners. I think the warden took appropriate action; this does not, however, alter the fact that DEA was required to release this information in the first place.

Mr. Brosan of DEA told the subcommittee that the Agency had also received requests for such things as its radio frequency, the tail numbers of its aircraft, their description, where they are stationed. He said that as of the time of his testimony, such requests had been denied. "However," he added,

I do not know whether we would be able to deny them if the requests were resubmitted at this time, due to some changes in policy . . . At the present time my understanding of the policy would be that we would have to demonstrate what harm could befall the Agency and its mission. If we could demonstrate that, then we would be able to withhold that data.

Repetitive requests

In supplemental responses submitted to the subcommittee, Mr. Bensinger said that there had been many instances of repetitive and duplicative requests. In one instance, DEA had received 32 FOIA requests from a single organization seeking information about itself. Each new request, related Mr. Bensinger, contained a list of names that the organization might be known by—sometimes as many as 25 names, and each new request reiterated a prior list already submitted, plus a couple of new names. This, said Mr. Bensinger, caused DEA to continually update and research its files, since each request had to be considered technically as a new request, encompassing all of the documents in the files up until the date of receipt of the request. The organization in question had filed a parallel number of requests with almost every agency of the executive branch. It had also filed FOIA lawsuits against virtually every agency of the executive branch. Defending themselves against these lawsuits has placed a heavy drain on DEA resources.

Investigative personnel rosters

Mr. Robert Chasen, U.S. Commissioner of Customs, testified that the Customs Service had received a request from the Women's Division of the American Civil Liberties Union for a roster of all female Customs inspectors. This roster, he said, was made available to them.

It developed, in the course of the questioning, that Customs had also released the names of all Criminal Investigators (GS-1811) as well as general investigators (GS-1810) who do some criminal investigative work among other chores. The exchange on this point merits quotation:

Mr. SHORT. Mr. Chasen, how do you handle personnel rosters at the present time? Do you disclose the investigators—the 1811's—as well as the others? Do you disclose the identities of your criminal and general investigators, or is that withheld?

Mr. CHASEN. I will let Bob Dickerson answer that.

Mr. DICKERSON. We disclose it if we are requested to disclose the name of an 1811 investigator. The name is disclosed.

Mr. SHORT. They are not withheld at all?

Mr. DICKERSON. They are not withheld.

Mr. SHORT. The total personnel roster of Customs is available under the Freedom of Information and Privacy Acts?

Mr. DICKERSON. That is correct.

Mr. LEHMAN. If I may, I would like to modify that in only one respect. Under the guidelines which the Civil Service Commission promulgated the only exception to this disclosure would arise in a case where it is requested for purely commercial purposes, such as to establish a mailing list to solicit business of some kind.

However, if, for example, we got a request from an organization which clearly was not going to utilize it for commercial exploitation we would be compelled to release it.

Mr. SHORT. When DEA testified—and I realize that they are under Justice and you are under Treasury—they stated that they were able to resist giving out the 1811 personnel rosters. I would just like to recommend that you talk to someone there, because apparently they do not interpret the law as being such. They can withhold this information.

While DEA had been able to resist requests for rosters of their GS-1811 investigators, they had not been so successful with their GS-1810 investigators. The questioning on this point with DEA follows:

Mr. SHORT. You have GS-1810 general investigators, don't you?

Mr. BROSNAN. Yes, Mr. Short.

Mr. SHORT. And they are required to perform a certain amount of criminal work?

Mr. BROSNAN. Absolutely. They are out there checking on the various drug firms and pharmacies and so on.

Mr. MARTIN. Have their names been revealed?

Mr. BROSNAN. Yes.

Senator THURMOND. Do you think it is wise to do that?

Mr. BROSNAN. No, sir. I would prefer not to reveal the names. We would prefer to withhold the entire list.

Senator THURMOND. Who forced you to reveal the names?

Mr. BROSNAN. We counseled with the Department of Justice by memorandum. We were advised at the last Freedom of Information Coordinators meeting last Thursday that it was discussed: We apparently have no legal grounds to withhold that information under the new civil service regulations.

Senator THURMOND. Under the Civil Service regulations?

Mr. BROSNAN. Yes, sir.

Mr. Chasen made it clear to the subcommittee that he was unhappy about such disclosures because "they are destructive of morale", and "could place our people in jeopardy".

Mr. Brosnan testified that in the case of his Agency it had so far been able to avoid releasing the names of its criminal investigators. When he was asked by Senator Thurmond whether DEA had received requests for rosters of investigative personnel, he replied:

We have had such requests, Senator. We have handled them by getting a computer printout of all our employees and then eliminating from that list those employees that are classified under the Civil Service classification of 1811, which is our criminal investigators. The balance of the list

has been forwarded to the requestor at the cost of the production, whatever that may be. It is \$20 to \$25 or something of that nature.

However, in response to a question submitted in writing, Mr. Bensinger told the subcommittee that "the refusal to disclose rosters of investigative personnel pursuant to (b)(6) exemption may not withstand judicial tests due to the use of the words 'clearly unwarranted'."

Mr. Chasen, in response to a similar question submitted to him, replied:

Civil Service Commission regulations require disclosure of certain information pertaining to employees, including name, grade, salary, duty station, and position title. There are obviously circumstances in which disclosure of this information could identify a particular agent involved in a particular investigation, including organized crime and narcotics investigations, as in the case of covert investigations. While every effort is made to withhold names of employees when disclosure would be a clearly unwarranted invasion of their privacy or might endanger them, the identity of a requestor as an organized crime figure or criminal is not always known. Thus, because criminals might identify agents or their families, agents are subjected to increased risk of injury or death from the disclosure of personnel rosters. Also, covert activities in such cases might be severely hampered or completely curtailed. Generally, a lower morale among agents would lead to lower quality and less efficient investigations.

Having said this, Mr. Chasen then confirmed to the subcommittee that harassment by anonymous elements is "not at all uncommon among agent personnel".

The release of investigative manuals

The Customs Technical Investigations Manual, or portions of it, was also released to two requestors under FOIA. Mr. Chasen noted that the Customs Technical Investigations Manual is intended for the use of Customs investigative personnel. Among other things, it outlines methods of dealing with various practical investigative problems. Among the other requests for manuals under consideration by Customs at the time of the hearing were:

- (1) A prison inmate has requested the "U.S. Customs Agents Manual";
- (2) A Topeka, Kans., high school student has requested the "Training Manual" used presently by Treasury Agents;
- (3) A California resident has requested the "Manuals of Instructions and Procedures for Customs Agents";
- (4) A California attorney has requested "Your Internal Regulations and Guidelines Pertaining to the Investigation of Criminal Matters";
- (5) National Treasury Employees Union has requested "A Copy of the Manual Used by Special Agents in Internal Affairs (Security)"; and

(6) A Washington, D.C., attorney has requested the "Customs Technical Investigations Manual, Inspectors Manual; and all finalized sections of Customs External Audit Manuals."

Other agencies also confirmed that they had received requests for investigative manuals.

The disclosure of investigative techniques and procedures

In addition to the uncertainty and concern over the release of investigative manuals, Mr. Bensinger said that DEA was also "concerned about our ability to protect from disclosure several sensitive, sophisticated investigative techniques used to protect undercover operatives and informants, and devices utilized in tracking suspects". Mr. Bensinger went on to note:

The (b) (7) (E) exemption allows us to withhold from disclosure any mention of these techniques or devices, provided that the reference to the device or technique is contained in an investigative file.

However, many of these techniques and devices were developed through the use of research contracts. The research files and the data contained therein relating to the development and use of the technique or device, is not an investigative file.

Therefore, although we will argue that the intent of Congress was to protect from disclosure these devices and techniques, the courts have shown a reluctance to accept "equity" arguments and claim our remedy is with Congress.

We have experienced similar problems regarding material we utilize in our training programs.

Any criminal who could gain access to the course material we provide during our training programs would have a decided advantage in avoiding apprehension and punishment.

We have received several requests for this type of material and we are unsure of our ability to defend against its disclosure due to the lack of specific language in the act which would protect it.

Release to foreign nationals

Several of the witnesses made the point that one does not have to be a citizen of the United States or a resident to obtain information under FOIA. They said that if they received such requests from foreigners resident in other countries, they would reply to the extent that they could, deleting only that information which they were entitled to delete under the various exemptions stipulated by FOIA.

"Shotgun" request

Mr. Bensinger also confirmed to the subcommittee that the Justice Department had received a request from a 15-year-old student who wanted the files in every unit and division in the department checked to see if they had information about him. He itemized each unit in the department to make sure that no file was overlooked. More than 100 employees of the Department of Justice, reported Mr. Bensinger, had to conduct searches of their files to respond to the request of this inquisitive minor.

Litigation

Spokesmen for Government agencies were agreed that litigation under FOIA and the Privacy Act seeking to compel the release of information denied to the requestors was already a very serious problem and that the number of cases under litigation was increasing.

Mr. Williams of IRS made the point that the very structure of FOIA encourages litigation by requestors, even when there is no question about the validity of the claimed exemption. He said that the burden of proof in any FOIA suit was on the defendant agency; and that when cases are brought to court, it has become commonplace for the courts to require agencies to submit detailed affidavits regarding the claimed exemptions in the case of each document or portions thereof.

In the case of IRS, said Mr. Williams—

Suits for access to investigative records predominate, again demonstrating the substantial impact this statute has had on the Service's overall enforcement effort. Almost 50 percent of the present FOIA litigation to which the Service is a party can be characterized as attempts by taxpayers to use the FOIA as a substitute for discovery.

In response to questions submitted in advance of the hearing, IRS informed the subcommittee that, as of January 12, 1978, it had a total of 77 FOIA/Privacy Act cases in litigation. Of the 84 cases that had already been decided as of that date, 20 were dismissed when the Government provided all or part of the documents which the plaintiff had requested; 34 cases were dismissed either by court decision or in consequence of the withdrawal of the complaint or of stipulations of one or both of the parties. Of the remaining 28 cases which had been decided on their merits, the Government had won 14, plaintiffs had won 8, and there were split decisions in 6.

In speaking about the continuing increase in the number of suits brought against the IRS under FOIA and the Privacy Act, Mr. Williams said that should large numbers of taxpayers who are subject to pending criminal proceedings institute actions of this type, IRS would find it difficult to meet the increased workload. Following up on this point, Senator Thurmond asked:

What would happen if, instead of having to defend yourselves against 68 simultaneous lawsuits—I believe this was the figure you gave for February 1978—you had to defend yourself against 10 times as many lawsuits nationwide, all at the same time? What would happen to the IRS?

In response to this question, Mr. Lester Stein, who accompanied Mr. Williams as a legal adviser, replied that IRS "would have no alternative but to throw in whatever resources are necessary and work with the Department of Justice to meet our obligations, because a criminal tax case must go forward. The Service will not readily cave in on its criminal tax program."

Speaking about the heavy burden placed on Government agencies by the requirement that every claim for an exemption must be justified to the satisfaction of the court, Mr. Stein further told the subcommittee—

More specifically, as the courts have pointed out, when the Government comes in and says that, under FOIA, to turn over the document would interfere with an ongoing proceeding, the court cannot take the word of the agency at face value.

Consequently, there are three general techniques that are used to establish to the satisfaction of the court, one way or the other, whether the Government's position has merit. As more than one court has indicated, none of these techniques are necessarily entirely satisfactory, but each one does involve a significant amount of time and effort. These are generally what the courts will require.

First, the court can ask for an in-camera inspection of the documents which the Government feels should not be turned over. This is burdensome. There are files that can be feet high. Courts are unwilling to go through these files and make a determination whether or not the disclosure of those documents would prejudice an ongoing investigation.

An alternative—as one of the circuit courts established—is to have the Government furnish an index of the documents that it does not want to turn over. The index generally will describe the document and its content without becoming too specific, because to become too specific would disclose the very document that the Government seeks to protect. The danger in the indexing is that, in some instances, this may furnish the prospective defendant the very information that he wants.

To index is a burdensome task, particularly if you have hundreds or thousands of documents, as is encountered in some cases.

A third alternative is for the Government to furnish affidavits or oral testimony describing what it has turned over to the individual who has made the FOIA request, and to establish, on the basis of affidavits, that the remaining material in the files is within the protection of FOIA.

Sometimes the Government approaches its task by relying on all three of these methods. Yet, it must establish, to the satisfaction of the court, that the documents it has should not be turned over to the defendant or to the taxpayer.

This is a difficult burden on the Government.

The Drug Enforcement Administration (DEA), in response to a written question, told the subcommittee that it had had a total of 40 cases in litigation since the enactment of FOIA/Privacy Act. The primary issues involved in this litigation seeking to compel DEA to release information had to do with administrative markings, invasion of third party privacy, and identification of law enforcement personnel. Twenty-one cases had reached final action status at the time of the hearing. DEA had substantially prevailed in every case with the exception of one, which was under a motion for reconsideration at the time of the hearing.

The collective testimony of the agencies which appeared before the subcommittee in the course of these hearings points to the conclusion that in many cases, Government agencies have avoided litigation by the simple procedure of caving in to requestors who threatened, or

initiated, litigation. Mr. Theodore Rojek, of U.S. Customs, told the subcommittee—

. . . as you perhaps know there is a requirement imposed on us by the Department of Justice that in any case in which the Agency is to deny a request under the Freedom of Information Act—if there is a strong indication that that denial will lead to further litigation, the denial itself must be cleared through the Freedom of Information Committee of the Justice Department. They do not always uphold or affirm the Agency's position.

THE CRIMINAL EXPLOITATION OF FOIA

Speaking in terms only slightly different from those employed by other witnesses, Capt. Justin Dintino of the New Jersey State Police posed this question about the effects of existing privacy legislation:

Who benefits from this situation? Certainly not the American people. The only real beneficiaries are the criminal and terrorist and other conspiratorial elements in our society.

Testifying in equally bitter terms, Chief James Powell, of the U.S. Capitol Police, said:

We have, by the enactment of the whole network of freedom of information and privacy measures at all levels created new elements in the bureaucracy: commissions, review panels, freedom of information specialists, reports, forms, and red tape. And to what purpose? Who is protected? Are the privacy and freedoms that we all cherish better protected by these controls? I am convinced that they are not.

Mr. Olszewski (former Director of IRS Intelligence) testified that, as the privacy laws stand today, the primary beneficiaries have not been our dissenters, but our mobsters and drug traffickers and other criminal elements. He added the following comment:

I must hasten to add that a relatively few, and I must emphasize a few, well-intentioned dissenters may have been improperly abused by some law enforcement information-gathering activities. However, the solution to these problems, as I said in my statement, is not to discontinue all information gathering, but to correct the misuse or abuse of the process where it may be found. If an auto manufacturer finds a fault in a number of vehicles caused by their manufacturing process, they don't discontinue manufacturing cars—they correct the error. The public is entitled to the same types of protection. Correct the mistake but don't disarm or emasculate law enforcement.

As Mr. Williams of IRS pointed out, one of the reasons why criminal elements have found it easy to exploit the privacy legislation is that "neither the FOIA nor the Privacy Act require a requestor to provide

personal information about himself or herself in making a request, nor do they require an explanation or justification of such requests".

On the subject of organized exploitation of FOIA/Privacy Act by the criminal world, the following exchange took place with Mr. Silberman:

Mr. SILBERMAN. If I may, let me tell you something about the underworld which you will be particularly interested in. The Bureau is enormously concerned because certain techniques have developed to, if I may use the term, to "play" the Freedom of Information Act/Privacy Act on the part of organized crime figures.

Senator HATCH. Does this include foreign espionage agents?

Mr. SILBERMAN. Yes.

Senator HATCH. Would you cover both of them?

Mr. SILBERMAN. Yes. It is a simple technique. Let's suppose that you are the head of a criminal conspiracy and you are concerned about the possibility of informants within your conspiracy—one or more. Therefore, you direct all of them to make Freedom of Information requests for their files.

First that puts the Bureau in a difficult position because they may or may not want to disclose that there is a criminal investigation which would permit an exemption. Suppose they had not started a criminal investigation yet?

Beyond that, there is a separate problem. The informant will not have a file. However, if they respond to everyone and say that the informant does not have a file, that is a dead giveaway that that individual making the request is indeed an informant. In that case, they have to make up a phony file in order to protect his identity. That is tricky.

Several of the witnesses made the point that when an FOIA request is submitted involving an open investigatory file, even if the agency is not compelled to surrender the information, the difficulties involved in processing the request, by themselves, would tend to disrupt the investigation.

The damage done when a violator discovers prematurely that he is under investigation was also discussed by Mr. Williams of IRS. In dealing with the detrimental effects of FOIA to the enforcement activities of his Agency, Mr. Williams said:

One area is that of substantive tax proceedings which may be complicated or thwarted altogether when a related FOI Act request results in the premature discovery of case related materials. Since investigation case files are likely to include information which is not exempt from the disclosure mandates of the FOIA, material is sometimes released which would not normally have been available to the subject of the investigation until the appropriate discovery procedures had been invoked during the course of litigation, and possibly not available at all.

Witnesses also testified that criminal violators can benefit from the Freedom of Information Act in three different ways. First, they can use the act as a discovery tool to find out what is in their files.

Second, if arrested, they can use the FOIA to drag out their cases in the courts. Third, if convicted, they can use it to suspend or delay penalties already imposed, by filing FOIA requests.

Commenting on this last legal device, Mr. Chasen of U.S. Customs testified:

Although disclosure in such cases may be denied in full or in part as determined on a case-by-case basis, the records frequently have to be copied or transferred to the Freedom of Information and Privacy Office to determine disclosure or exemption.

This alone causes interference and delays in the investigation and processing of the actual cases. In addition, this transfer creates attendant security risks since the case agent must cease the investigation, copy the data already compiled, and await a response from headquarters as to the scope of the disclosure, if any.

The mere act of filing a Freedom of Information request is in itself a valuable and foolproof instrument of discovery for criminals seeking to find out if anything is known about their current criminal activities. On this point, the following exchange took place between Senator Thurmond and Mr. Bensinger of DEA:

Senator THURMOND. I believe you mentioned the case of a drug suspect, then under active investigation, who requested information about himself from your files. Had you replied that you had no information, you would have been in violation of the law. Had you told him that you had information but you could not release it to him, you would have been alerting him to the fact that he was under investigation.

Your testimony was: "Fortunately, by the time our Freedom of Information Office could act, the subject had been arrested and the hashish confiscated."

What if there were no such fortunate delay? How could you handle a request from a suspect under active investigation without either violating the law or alerting him?

Mr. BENSINGER. I think this is a principal problem, Mr. Chairman. I want to frankly express a concern with that.

If the suspect is under investigation, we respond and say that we cannot release the data to you in our systems of records that you request, because it is not available.

If the person is not under investigation, according to Mr. Brosan, the response is, "We have no information on this individual."

While the sentence that I read to you with respect to not providing the information in the systems of records and it not being available is what is said, this is a red flag to a drug trafficker.

In response to a question asking whether U.S. Customs had received requests for information under FOIA from criminal elements, the Customs Service responded that it "has received requests for information under the Freedom of Information Act from persons

believed to be major organized crime figures or racketeers on whom Customs had conducted investigations." The Customs Service went on to say—

Major violators who submit requests receive the same consideration as any other requestor. A co-conspirator in the notorious 1971 French Connection narcotics smuggling case was arrested by Customs Special Agents for causing to be smuggled and distributed into the United States some 200 lbs. of pure heroin, and conspiring to smuggle and distribute an additional 500 lbs. of the drug. The individual was tried, convicted and imprisoned. A one line request from him, which was processed under FOIA, resulted in 35 or 40 documents contained in his investigative file being disclosed to him.

FOIA: OTHER ADVANTAGES TO THE CRIMINAL WORLD

The testimony established that the criminal world has benefited in other important ways from the FOIA and Privacy Act.

Informants

All of the witnesses from the law enforcement field emphasized the importance of informants to any effective law enforcement intelligence program. They were equally emphatic on the point that FOIA had virtually wiped out their ability to recruit informants or to obtain citizen cooperation.

"Without informants," said Mr. Silberman, "criminal law enforcement is impossible." He went on to say:

Former associates in the Bureau have told me that informants have been literally frightened by the knowledge that under Freedom of Information Act/Privacy Act requests these risks do occur. As a result, there have been several occasions where informants have requested the Bureau to destroy everything in the file which relates to them. Indeed, their activity in providing information of law enforcement importance has been chilled. I can't blame them.

* * * * *

There are other instances of this. One example I should give you is one that was given to me by former associates in the Justice Department. It is a situation where a businessman faced with criminal activity in his business wished to allow Federal agents to be placed in the business in order to discover the criminal activity. However, he was afraid to do so for fear that through Freedom of Information/Privacy Act disclosures it would come out that he had cooperated with the Federal Government.

Without citizen cooperation, law enforcement is impossible.

Let me go on to say that I am aware of other instances where, by virtue of the impossible task that has been imposed on the FBI, intelligence information—in one case foreign intelligence information and in other cases criminal law intelligence information—has been disclosed.

In those cases, people cross their fingers and hope that no one will put together the information which is disclosed with other information and come up with a conclusion which would be deleterious to our capability.

There may be those who will say, "Well, there is human error in everything." However, what is so important about this is that this impossible, horrendous task that has been imposed on the Bureau of a document-by-document analysis of each of the files, which are subject to Freedom of Information Act or Privacy Act requests, will inevitably and inexorably lead to these kinds of errors which will identify informants and which will chill the capability of the intelligence operation.

* * * * *

. . . with the massive task which the Bureau has, it is absolutely inevitable that human error will result in the disclosure of information that should not be disclosed.

* * * * *

The important thing is that these mistakes are inevitable given the scope of the requests and the necessity which Congress placed upon the Bureau to make a page-by-page analysis of investigatory files in order to determine what should and should not be disclosed.

One of the reasons that it is inevitable that there will be mistakes is that the people doing that analysis are not going to be the same people who are doing the investigation. Therefore, they may not know what kind of information will trigger, in the wrong hands, the disclosure of the identity of informants.

Backing up what had been said by other witnesses about the attrition of the informant program, Mr. Quinlan J. Shea of the Justice Department noted: "if an individual thinks he is going to get sued civilly for damages by furnishing information to the FBI, simply having an FBI agent tell him that it is not so, or probably is not so, will not do much good."

Mr. Shea's statement did not go quite as far as it might have gone. It is a matter of common knowledge that revealing the identity of an informant, especially in the case of organized crime, can frequently place his life in jeopardy. And, as Mr. Silberman testified, informants lives already have been placed in jeopardy by the inadvertent release under FOIA of information which served to identify them.

To the credit of our law enforcement agencies and personnel, they have been doing their utmost to protect the identity of informants, in the face of a number of court decisions heavily weighted in favor of the absolute privacy concept. Chief Powell of the U.S. Capitol Police told the subcommittee of one such case involving a law officer from Chicago with whom he had recently attended a FBI symposium. The law officer in question, said Chief Powell, was under court order to reveal the name of an informant, but he had refused to do so. Although the officer was concerned that he might have to go to jail for his attitude, he remained determined not to furnish the name of the informant because this could lead to his death or serious injury. This was something, he felt, that no police officer should be compelled to do.

The shattering impact of FOIA on the law enforcement informant program nationwide is dramatically apparent from the fact that, whereas in 1975 the FBI had some 1,100 informants monitoring the activities of terrorist and extremist groups, both far left and far right, by July 1978, according to its own statement, it was down to 42 informants for the whole of the United States. In releasing the FBI's Uniform Crime Report on September 14, 1978, Attorney General Griffin B. Bell frankly discussed the damage done to the FBI's informant program by FOIA, and he suggested that the law be amended by exempting criminal investigative files from disclosure for a period of 10 years.

The freeze on sharing intelligence

There was also unanimous agreement on the part of the witnesses that the Freedom of Information Act had had a disastrous impact on intelligence gathering capabilities generally and that it had restricted, almost to the point of freezing, the sharing of intelligence between local and State agencies and Federal agencies. Organized crime, needless to say, has also benefited from this paralysis.

Discussing this situation, Mr. Glen King of IACP testified:

Although neither the Freedom of Information Act (FOIA) nor the Privacy act of 1974 apply directly to State or local law enforcement agencies, both acts have impacted strongly on the intelligence-gathering capabilities of State and local law enforcement agencies.

The impact comes from four major sources. They are: (1) confusion over the interpretation of the acts as well as the extent to which they require agency adherence; (2) State and local laws enacted pursuant to the FOIA and Privacy Act; (3) lawsuits brought against law enforcement agencies under the acts; and (4) adverse media coverage of law enforcement intelligence activities.

As you know, the 1974 amendments to the FOIA changed the then existing law which exempted from disclosure law enforcement files compiled for investigatory purposes or investigatory files compiled for law enforcement purposes. The restrictive guidelines of the 1974 amendments have forced local and State agencies to perform exhaustive analyses on the files to determine what was disclosable. State and local law enforcement agencies have been deterred in the transmission of intelligence information to Federal agencies for fear that the Federal agencies will be required to disclose the information under the FOIA. The use of informants and confidential sources has been chilled for fear their identities will be disclosed.

Police intelligence access to Federal records has also been restricted by the Privacy Act of 1974. The act prohibits the disclosure of any information on an individual maintained by a Federal agency in a system of records unless permitted by a specific exemption. Although there is an exception for certain law enforcement purposes, a significant amount of confusion has developed regarding implementation of the act. Many law enforcement intelligence officials are of the opinion that it has restricted access to needed intelligence data.

As a concrete example, Mr. King described a report he had recently received from the Washington State Patrol. The report said that, because the FBI could no longer conduct surveillance operations except in open investigative cases, the patrol no longer has access to the kind of criminal information that previously was made available to it by the Bureau on a routine basis. The report said that on two occasions, organized crime figures had travelled into the State of Washington and the police agencies there had known nothing of their presence in the State until after their departure. The report noted that, prior to the enactment of FOIA and the Privacy Act, such movements would have been monitored by the FBI and law enforcement agencies in the State of Washington would have been alerted.

The damage done has been compounded by the fact that many States have enacted freedom of information laws and privacy laws of their own, some of which impose even more stringent restrictions than the FOIA/Privacy Act. Discussing the difficulty which this complex of restrictive laws has created for his Agency, Mr. Chasen of the U.S. Customs testified:

In a given case, Customs may not be able to safeguard information from a State in compliance with its privacy laws or our agreement with it because such information has become part of our intelligence files, and therefore falls within the purview of Federal disclosure laws which may be less stringent than the States'. More importantly for Federal law enforcement purposes, a State may recognize this reality and choose not to provide information to the Customs Service.

As important as it is for a Federal agency to receive and make use of information from State and local law enforcement agencies, we recognize that it is equally as important that State and local agencies have access to intelligence in the files of Federal agencies.

In the past, the Customs Service has routinely provided such information to State licensing and regulatory agencies to enable them to carry out their respective functions. However, the flow of information from Federal agencies has been impeded by the restrictions in the Privacy Act as to what may be disclosed

The impact on international law enforcement intelligence

The witnesses testified that FOIA has also placed serious difficulties in the way of continued cooperation with law enforcement agencies of other countries, in monitoring criminal activities of an international nature.

Mr. Bensinger of DEA told the subcommittee that, in negotiations with law enforcement authorities in Britain and France, these agencies had made it very clear that they would refuse all future cooperation if their American counterparts could not guarantee absolute confidentiality of third-party information received from other countries. In one court case, said Mr. Bensinger, the judge had upheld DEA in claiming exemption for such information. "Had the ruling been otherwise," Mr. Bensinger added, "that is, had it been established that we were obligated to disclose information provided to us by foreign, State or local authorities, I think I can safely say that the impact of the Freedom of Information Act on DEA's effectiveness would have been devastating."

The matter of agreements with law enforcement agencies in other countries was also the subject of the following discussion with the witness from the U.S. Customs Service:

Mr. SCHULTZ. You said in your statement that mutual assistance agreements with law enforcement agencies in other countries now must include language that the agreements are subject to Federal legislation which might require disclosure of information. Is this a requirement of the Freedom of Information Act or the Privacy Act?

Mr. ROJEK. The reason that we include it is that these type of agreements fall into the category of "executive agreements". They are not like a treaty. Therefore, being unlike a treaty and being merely an executive agreement, they are subject to all domestic laws, including laws such as the Freedom of Information Act and the Privacy Act.

During the course of those negotiations, of course, our counterparts were aware of the restrictions and the limitations as well as the requirements that we may have to disclose. While these agreements at this time have had language put in that is designed, supposedly, to carefully guard whatever information they give us, we have been put on notice that in the event that those agreements in that respect are abridged, it will be more difficult for us to reach a similar agreement the next time around.

Obviously, there is no way of quantifying the damage that has been done to cooperation with law enforcement agencies in other countries. But the several witnesses who addressed this matter were convinced that much damage had already been done by the growing fear that U.S. agencies could not protect intelligence that was shared with them.

RECOMMENDATIONS FOR AMENDMENTS TO THE FREEDOM OF INFORMATION ACT AND THE PRIVACY ACT

The practical experience with the Freedom of Information Act and the Privacy Act over the past four years points to the need for a whole series of amendments designed to restore the balance between the right to privacy and the right to know, on the one hand, and the right to personal security and the requirements of national security, on the other hand.

Some of the suggested amendments are relatively simple and it will, hopefully, be possible to achieve a consensus on these amendments with little controversy. Among such recommendations are the following:

(1) The requirement that substantive replies to requests under FOIA be mailed within ten days is completely unrealistic and should be amended to provide Government agencies with sixty days response time.

(2) Rosters of investigative personnel or of employees in sensitive Government agencies or sensitive positions should be specifically exempted from disclosure.

(3) Government agencies should not be required by law to process requests under FOIA coming from foreign nationals.

(4) The law should be amended in a manner which specifically guarantees the confidentiality of all information received from foreign governments by exempting such information from disclosure.

(5) Law enforcement training manuals, investigative handbooks, and manuals dealing with investigative technologies developed through confidential research contracts, should be specifically exempted from disclosure.

(6) In the interest of reducing the harassment and labor drain resulting from repetitive requests, applicants for information under FOIA or PA should be required, when asking for information about themselves or any specific subject, to state the number of such requests they have previously made, if any, and provide the dates of these requests. Congress might also wish to consider the advisability of limiting applicants to Government agencies to a maximum of one request per year per agency on any given subject, with the additional stipulation that responses to new requests from the same applicant simply bring the previous response up-to-date, rather than repeating the entire contents of the file.

(7) Where public record items such as newspaper clippings and court records are incorporated in the file, the agency should not be required to xerox these for the requestor, but should, instead, simply be required to identify these items by date and source.

Amendments will also be required to undo the current paralysis on the free exchange of intelligence between law enforcement agencies and to restore the confidence of informants of all categories and of our citizens in general that their cooperation with law enforcement will not result in the disclosure of their identity.

1. To break down the paralysis in the exchange of intelligence, an amendment is required that would protect information provided by third agencies from automatic disclosure. Conceivably this could be accomplished by vesting the burden of disclosure with the originating agency, so that they would remain in effective control of their own intelligence. The alternative to such an amendment is the indefinite continuation of the present paralysis, with pyramiding consequences for our law enforcement community.

2. Some legislative formula also has to be found that would not make it mandatory for our Federal law enforcement agencies, in withholding information from active investigative files, to inform the subjects of these files that they are, in fact, under active investigation. This might be accomplished by providing for the automatic exemption from disclosure or acknowledgement of any investigatory material compiled within a number of years of the date of request. FBI Director Webster has suggested that investigative files be exempted for a period of ten years. This is not an unrealistic period of time when one considers the very large number of criminal cases that can only be brought to court after years of investigation. By informing requestors in advance that all investigative files are automatically exempted from disclosure or acknowledgement for a period of X years, Government agencies could be extricated from the dilemma of having to acknowledge the exist-

ence of an active investigation, if there is one, or having to engage in dilatory tactics or having to perjure themselves if they consider it essential to conceal from the subject the fact that he is under active investigation.

3. Finally, some formula must be found for an amendment that will provide far more effective protection for informants and cooperative citizens than is currently the case. Exempting investigative files from disclosure for a period of ten years, as suggested in the previous section, would be helpful. But more than this will be necessary. The present requirement that investigative files be gone through on a page-by-page, paragraph-by-paragraph, word-by-word basis, not only places an exceedingly onerous burden on the custodian agency but also enhances the possibility that informants will be identified through the release of a combination of items that enable the subject of the file to zero in on the source. An amendment that effectively protects the identity of informants or cooperative citizens almost certainly involves a quantitative retreat from the concept of maximum possible disclosure. But it should be possible to do so without compromising the public's right to know in any serious manner.

The alternative to such an amendment, again, is a continuation of the present constraints on law enforcement which effectively deprive them of the time-honored and vital intelligence instruments of informants and public cooperation.

VII. FACTORS CONTRIBUTING TO THE EROSION (III): IMPACT OF THE TAX REFORM ACT OF 1976

Certain provisions of the Tax Reform Act of 1976 have also contributed to the erosion of law enforcement intelligence and to the growing restrictions on the sharing of intelligence by law enforcement agencies. This was established in the replies of the Internal Revenue Service (IRS) to a long series of questions submitted to them subsequent to the hearing of April 25, 1978.

Section 6103 of the Tax Reform Act of 1976 placed severe restrictions on the disclosure to other law enforcement agencies of non-tax information developed in the course of a tax investigation.

In response to a question, IRS replied that section 6103 had had "no significant demonstrable adverse effect with respect to the ability of the Criminal Investigation Division to develop criminal tax cases."

However, when IRS was asked to what extent this legislation had affected the willingness of other law enforcement agencies to share information of potential use in tax cases with the IRS Intelligence Division, they replied:

Some law enforcement agencies have been reluctant to share information with IRS. In at least one Internal Revenue Service District, our Criminal Investigation Division personnel have been excluded from meetings attended by representatives of State and other Federal law enforcement agencies held to discuss organized crime and to exchange general intelligence information. These other agencies voted to exclude Internal Revenue Service personnel since we can only provide information within the confines of the disclosure restrictions contained in Section 6103.

In response to another question, IRS stated that it is strongly committed to a narcotic traffickers strike program and that the disclosure law requirements had no effect on their desire to work with this program. In response to the very next question, however, IRS said: "Under current disclosure statutes we do not participate in the target selection process since we cannot disclose taxpayer identifying information to the Strike Force Attorney at that stage in the investigation."

Although IRS told the subcommittee that it seeks to cooperate in sharing information relating to Federal Criminal Law violations with other law enforcement agencies, it was frank in admitting that in many cases it could not share such information, even where fairly serious violations were involved. In general, it appears that IRS feels free to share information about criminal law violations when this information comes from third party sources unrelated to the taxpayer; while its

construction of the limitations under section 6103 is that it cannot share information when this comes from taxpayer records or tax returns or admissions or submissions. At the request of the subcommittee IRS submitted a list of 42 possible Federal violations which were not referred to the relevant law enforcement agencies because of these limitations. Among the cases not referred, were five cases of possible bribery of Federal officials, six cases of securities law violations, fifteen cases of possible illegal political contributions, and a variety of other violations of the Federal laws. In consequence of nonreferral, obviously these criminal violations of the law all went unpunished.

The Tax Reform Act of 1976, Title 26, Section 7609, established stringent regulations governing the release of third party information. Describing these requirements, IRS said:

The Tax Reform Act of 1976 placed the requirement that the Internal Revenue Service notify, in writing, the taxpayer when a summons is served on a third party record keeper (as defined in the Act). This notice informs the taxpayer of his/her right to stay compliance of the summons and the procedure he/she must follow to do so. It also provides him/her with a copy of the summons. The Act further placed the requirement that the Internal Revenue Service provide the notice to the taxpayer within three days after the service of the summons. The taxpayer has fourteen days after the receipt of the notice to stay compliance, during which time the Service may not examine the summoned records.

Commenting on the overall impact of these requirements, IRS said that "reports from the field indicate that a number of subjects of criminal inquiry, including tax protestors, have seized upon this as a means of delaying investigations, knowing that as time passes records become lost and potential witnesses die."

When asked what benefits had accrued to the taxpayers as a result of the revised summons provisions of the Tax Reform Act, IRS replied that for the period March 1, 1977-March 31, 1978, 478 summons challenges under section 7609 had been decided by the District Courts in favor of the Government, while their survey could not find a single summons case in which the court had ruled against IRS during the same period. "These figures," said IRS, "seem to indicate that the section 7609 procedures are not protecting any legitimate interests of the taxpayers but are merely delaying legitimate investigations by the Service."

The testimony revealed that, even where taxpayers do not initiate legal action to stay compliance with the summons, the Tax Reform Act of 1976 has had a chilling effect on the willingness of banks and other third party sources to comply with IRS summonses. IRS told the subcommittee that during the period of March 1, 1977 to December 20, 1977, various banks have refused to comply with IRS summonses in a total of 77 cases.

The point that must be made in summarizing this testimony is that the restrictions imposed under the Tax Reform Act of 1976 not only impairs IRS's ability to investigate and deal with criminal violations of the tax laws, but have a constrictive effect on the entire field of law enforcement by hobbling the ability of IRS to share information with other agencies and to participate with them in joint strike force activities directed against drug traffickers and other criminal elements.

VIII. CONSEQUENCES OF THE EROSION (I): THE CRIPPLING OF ABILITIES TO DEAL WITH TERRORISM AND CIVIL DISTURBANCES

TERRORISM

Acts of terrorism over the past decade in this country have cost scores of lives and inflicted property damage running into the many millions of dollars. In addition, there have been numerous attacks on law enforcement officers by so-called urban guerrilla terrorist groups, which, according to the FBI, for the period 1971-76 alone, resulted in the death of 43 officers and the wounding of 157 more.

A few of the many hundreds of acts of terrorism have been widely publicized and are therefore generally known to the public. Among the incidents which received the greatest attention were the bombing of the Mathematics Building at the University of Wisconsin during the anti-Vietnam protest movement, which did millions of dollars worth of damage and blew a 31-year-old graduate student to bits; the LaGuardia bombing of December 29, 1975, which cost the lives of 11 and injured another 51 people; the Fraunces Tavern bombing in New York City on January 29, 1975, which cost the lives of 4 people and injured 53.

But there have been countless other incidents which were not called forcefully to national attention or which have been forgotten. Following are several of the many such incidents listed in the "Defenseless Society" which was submitted for the records as an exhibit by Mr. Frank Carrington:

In October 1972, six members of the "De Mau Mau" gang, a racist terrorist group, were arrested in Chicago for the execution-style murders of nine persons in the Chicago area.

* * * * *

Two white youths were murdered in Jacksonville, Fla., in June 1974. The Black Liberation Army claimed credit for the killings, stating in tapes sent to local TV stations that "more white devils will die".

* * * * *

After the arrest of Lynette Fromme for the attempted assassination of President Ford, her roommate, Sandra Good, also a member of the Charles Manson cult, told reporters that some 75 business executives and their wives had been marked for torture and death by the "International Peoples Court of Retribution" for polluting the environment.

Mr. Carrington also pointed out that while the public recalls the conviction of the Manson Gang on the charges of murdering Sharon Tate and six friends in Los Angeles in 1968, the actual number of murders committed by the gang may have run as high as 35.

But all of this is past history. The many witnesses who testified before the subcommittee on the question of terrorism were unanimous

on the central point that the country was bound to see a continuing escalation, quantitatively and qualitatively, in the phenomenon of terrorism in the coming years. They were also agreed that without effective intelligence there could be no meaningful defense against the growing number of terrorist groups that were threatening the security of the country. Finally, they were unanimous on the point that they do *not* have effective intelligence today and that they are handicapped and restricted in so many different ways that, as one anti-terrorist specialist put it, they are always in the position of "playing catchup ball".

They testified that they have in recent years been deprived, or virtually deprived, of all of the instruments essential to effective intelligence.

There is very little intelligence left at local, State or Federal levels, and what little remains is not freely shared with other law enforcement agencies, despite the highly mobile nature of terrorist groups.

Informants, thanks to the Freedom of Information Act and recent court decisions and restrictions, are on the verge of becoming an extinct species.

Electronic surveillance is completely forbidden in 21 States and can only be used under extraordinary circumstances and pursuant to a court order in virtually all of the remaining States.

Access to telephone records and other third-party records by law enforcement agencies now generally requires court orders and in some states requires that the subject be notified—all of which may completely vitiate an investigation when the need is for immediate access to records in order to prevent a crime or make an arrest.

The various witnesses on terrorism stressed the following basic facts about terrorist groups:

- Terrorist groups are highly conspiratorial and highly mobile.
- A number of these groups have had contact with unfriendly foreign governments.
- They have an ideology which in most cases weds terrorism to traditional Marxism.
- They are highly sophisticated and becoming more sophisticated.
- Their numbers are growing.
- They frequently cooperate with each other.

The best known groups in recent years have been the Symbionese Liberation Army, the Weather Underground Organization, the New World Liberation Front, the Red Guerrilla Family, the Black Liberation Army, the Chicano Liberation Front, and the Puerto Rican FALN (Armed Forces of National Liberation). But there are scores of other groups and grouplets whose names are not generally known to the public but which have been actively involved in terrorism. In addition to these openly terrorist organizations, there have been other organizations or associations which have functioned in the public domain as support groups for terrorist organizations. This, for example, has been the relationship of the so-called Prairie Fire Organizing Committee to the Weather Underground and of the Castro-inspired Puerto Rican Socialist Party to the FALN.

The common ideology shared by most terrorist groups is manifested in their common reverence for the major theoreticians of modern terrorism like Raoul Sendic, of the Tupamaros of Uruguay, and Carlos

Marighella, the Argentinian terrorist. It is also manifested in the basic texts which the members of all terrorist groups study, with a fervor and devotion that good Christians reserve for the Bible.

The basic strategy of urban terrorists was spelled out in these words by Carlos Marighella in his work, "The Mini-Manual of Urban Guerrilla Warfare," which, incidentally, was printed in a number of languages and internationally distributed by the Castro Government—

Within a firing group there must be complete confidence among the comrades. The best shot, the one who best knows how to manage the machinegun is the person in charge of operations. The firing group plans and executes urban guerrilla actions, obtains and guards arms and studies and corrects its own tactics, so when there are tasks planned by the strategic command, these tasks take preference, but there is no such thing as a firing group without its own initiative.

For this reason, it is essential to avoid any rigidity in organization in order to permit the greatest possible initiative on the part of the firing group.

The theoretical works almost invariably found on the bookshelves of our domestic terrorists are supplemented by sophisticated handbooks on the manufacture and use of improvised explosive devices and firearms. In the early days of the American terrorist movement, the so-called "Anarchist Cookbook" was one of the texts most commonly found. In recent years, however, terrorists have managed to upgrade their instructional manuals by printing and distributing highly classified works on the subject compiled for the use of the CIA and Special Forces. For example, Desert Publications, an underground printing house in Phoenix, Ariz., has been advertising "The Complete C.I.A. and Special Forces Black Books—Improvised Munitions Handbooks". "These books," said the advertisement, "were originally developed by Frankford Arsenal for CIA and Special Forces. They are the most detailed and comprehensive works ever done on the subject of improvised weapons. For years they have been the most sought-after and secretive books ever published by the American military."

The advertisement wound up with these ominous words: "Anyone who can foresee the troubled times ahead should not be without the knowledge contained in these books."

Up until now, terrorism has been limited to traditional manifestations like shootings, bombings, and kidnappings. There is no reason to believe, however, that the terrorists of the future will be quite so "conservative". There is general agreement among experts on terrorism that future years will witness instances of bacteriological terrorism, nuclear terrorism, and terrorism employing or threatening the use of exotic instruments like nerve gas. Sgt. Arleigh McCree, the officer in charge of the Los Angeles Police Department Bomb Squad, told the subcommittee in October 1975 that he had at that time already investigated four threats to produce and use nerve gas.

The threat of nuclear terrorism

Several of the witnesses who testified on terrorism before the subcommittee spoke of the danger of nuclear terrorism. This has already been the subject of a number of studies by Government agencies and think-tank organizations.

There is the possibility that terrorists might be able to seize a nuclear facility and threaten its destruction if their demands are not met.

There is also the possibility that terrorists or their accomplices might, over a period of time, be able to steal the two kilograms of plutonium (about 4½ pounds) necessary to make a "basement bomb". An Atomic Energy Commission study pointed out "there is a growing body of persons, with scientific training or experience in the nuclear power industry, who could make a bomb." Dr. Mason Willrich and Theodore B. Taylor, who prepared a study for the Ford Foundation, said that crude fusion bombs could be built "using materials and equipment that could be purchased at a hardware store and from commercial suppliers of scientific equipment for student laboratories."

Finally, there is the possibility that nuclear terrorists might use a few ounces of plutonium to poison water or to poison the air in a large building by introducing it into the airconditioning system. In their widely distributed work, Willrich and Taylor pointed out that Plutonium 239 "is at least 2,000 times more toxic than cobra venom or potassium cyanide, and 1,000 times more toxic than heroin, or modern nerve gases." It was their estimate that ingesting 2-millionths of an ounce of plutonium would be fatal.

There are some of the possible scenarios the United States and other Western nations may have to confront in the not-too-distant future. But against such possibilities, we have virtually no preventive defenses because of the mayhem worked on our law enforcement intelligence resources and because of the related inability to do background checks on workers in non-military nuclear facilities.

The role of intelligence in combatting terrorism

As was pointed out previously, the many witnesses who have testified before the subcommittee on the subject of terrorism emphasized the importance of law enforcement intelligence in the strongest terms.

Mr. Brian Crozier, Director of the London Institute for the Study of Conflict, in his testimony of May 24, 1975, told the subcommittee—

Intelligence is of the utmost importance. It is necessary to collect and collate the intelligence which is available normally to a wide variety of agencies. . . . All these forms of intelligence must be centrally collated and there must be a coordination of the anti-terrorist effort.

At the same hearing, Mr. Robert Fearey, who was in charge of the State Department's Task Force on Terrorism, testified that intelligence was "a *sine qua non* of any effective action," and that we must have "adequate intelligence about existing terrorist groups and individuals, their present and past activities, methods of operation, and all contacts among them."

A study on antiterrorist measures put out by Mr. Crozier's organization further underscored the importance of the sharing of intelligence. In its section on "International Action," it said:

Each country's police accumulates a mass of data, including statistics on terrorism. Much of it can be computerised. All European countries should compile profiles of terrorist groups and individuals. This information should be pooled or at all events made readily available to other police forces needing information.

Chief Davis, of the Los Angeles Police Department, in his testimony of September 9, 1976, gave several examples of how effective intelligence on extremist organizations had been able to thwart their plots:

Chief DAVIS. One of the most significant things that comes to my mind is that a local judge, Alfred Gittelsohn, a few years ago issued a school desegregation order, which was not universally popular in Los Angeles County. And one of my undercover men working to find out what rightwing terrorists were up to—we cover the whole spectrum—was hired by a man to murder Judge Gittelsohn and then to write a note saying, "This is for the Jews," and with a spike, drive this into the forehead after he had murdered Judge Gittelsohn. Now, the price of this murder was \$500 and, of course, fortunately it was a Los Angeles police officer who was hired and we were able to prosecute and send this man at least away to a mental institution. Now, if we had not been doing the intelligence gathering function there, we would have been in serious trouble and I'm sure the judge might well not have been with us.

Mr. SCHULTZ. Chief, just for a clarification on the record, when you say "fortunately it was a Los Angeles police officer who was hired," please clarify that so we don't misunderstand the import of your statement.

Chief DAVIS. Well, a Los Angeles police officer was assigned to gather intelligence data on dangerous, disruptive, rightwing organizations. And obviously when he was solicited to commit this murder, we felt that we had to bring him out from his undercover role and go forward with the prosecution.

Mr. SCHULTZ. Thank you.

Chief DAVIS. Now, another classic example: In the early 1970's when the Brown Berets in Los Angeles were a very volatile group, again I had a member of my department, who was very compatible with that organization—they didn't realize his background—and when Governor Reagan was giving a speech in the Biltmore Hotel in downtown Los Angeles, this Brown Beret group set several fires in the Biltmore Hotel. Because of my man's knowledge of this, he was able to see that the fire department was summoned and the fires were put out. They proceeded from the Biltmore Hotel to a Safeway store on the east side of Los Angeles and there they were going to undertake a detonation and explosion that did pose a threat to life and great property damage. And it was necessary at that point for my man to come out from cover and to make arrests of the Brown Berets involved in that particular operation.

All through the actions of the Brown Berets and other organizations trying to create difficulty in East Los Angeles and during some difficulties in essentially the Mexican-American area, the extent of our intelligence gathering there allowed us to go through that whole disorder—a series of disorders—without the loss of one life or without any injury in Los Angeles and without any substantial property damage. I think there was one 10-cent store burned down in Wilmington, California.

Now, without the day-to-day gathering and analysis and utilization of intelligence information on my part, we probably would have suffered substantial losses, maybe in lives and certainly a great deal of property damage.

The wipe-out of anti-terrorist intelligence capabilities

We have already dealt with the total destruction of the domestic intelligence capabilities of the Washington Metropolitan Police Department, which preceded and made possible the Hanafi Muslim seige. Such destruction of intelligence capabilities relating to terrorist groups has now become a widespread phenomenon. Another dramatic incident was the plight of the New York Police Department's intelligence unit at the time of the Fraunces Tavern bombing. Some years prior to this incident, Mayor Lindsay of New York had issued instructions that resulted in the destruction of the bulk of the intelligence files, including files on potential terrorist groups such as the FALN. When the bombing took place, the New York Police did not possess any meaningful intelligence on the FALN—with the result that they had to come to the Senate Subcommittee on Internal Security for background information. Mr. Frank Carrington quoted a detective assigned to the case as saying:

We haven't done any surveillance of Puerto Rican political groups for several years. We've been forbidden from even attending meetings as observers. The truth is that we have no good contacts inside the Puerto Rican community and we were completely unprepared for the FALN when it sprung up.

On the heels of the Fraunces Tavern bombing, 100 New York City policemen were assigned to the investigation of the FALN. But this investigation was seriously handicapped by the now widely accepted criterion that no intelligence entry can be made about an individual on the basis of "mere membership" in a group—that there has to be an indictment or a conviction against him before an intelligence entry can be justified. This exempted from the intelligence files virtually the entire membership of the Castroite Puerto Rican Socialist Party, which has openly endorsed many of the acts of terrorism perpetrated by the FALN, and several of whose members have been tied in with FALN bombings.

As early as October 1974, Director Clarence Kelly of the FBI, had spoken despairingly of "the inability of authorized law enforcement agencies to cope with terrorist acts."

Sgt. Arleigh McCree of the Los Angeles Police Department, an officer of the International Association of Bomb Technicians and Investigators, told the subcommittee in October 1975:

I do not want to appear to be on a tirade about it, but the various police intelligence agencies around this country—and I deal with them on a constant basis, since I am the information officer for the IABTI Association—intelligence is relatively nonexistent among the major police departments in this country today. I attribute that to a very effective counterintelligence campaign by the members of the New

Left themselves, and by, of course, some well-intended legislation.

Speaking further about the difficulties that law enforcement officers have in investigating terrorist groups, Sgt. McCree said:

For example, Senator Thurmond, if I go to an outfit like Pacific Gas & Electric or the telephone company, and ask who holds this particular telephone number, I may arrest a terrorist who may have the telephone number in his possession. If I try to check it back, many times the companies refuse to provide that information, because they don't want to be a party to lawsuits, or be accused of invasion of privacy, and these sorts of things.

Today the situation is much worse than it was in 1974 and 1975.

The terrorist intelligence apparatus

Sgt. McCree testified that, while law enforcement agencies were systematically destroying their intelligence about terrorists and terrorist support groups, the terrorists, on their side, were operating an increasingly effective intelligence network of their own. Most terrorist groups operate with limited membership, but even very tiny groups like the SLA have remarkably precise information about a broad range of potential targets, personal and corporate. Apart from the fact that the intelligence capabilities of some of these groups are manifestly far in excess of their own resources, the witnesses told the subcommittee that there was solid reason for believing that terrorist intelligence was fed by an army of leftwing research collectives, one of which, Resource One, was equipped with a high priced modern computer. The computer in question was described as an XDS-940 computer, a second-generation computer, with a storage capacity of approximately 67 million elements per disc. It was estimated that it cost approximately \$500,000 when new. Sgt. McCree testified that it had been purchased with contributions from corporate foundations—\$25,000 from the Bank of America Foundation; \$24,600 from the San Francisco Foundation; \$10,250 from the Firemen's Fund of America; and so on. He expressed the opinion that the donors were unaware of the use to which their contributions would be put.

In support of these statements, it should be noted that the subcommittee had received from a previous witness, California Attorney General Evelle Younger, a copy of the SLA (Symbionese Liberation Army) "hit list", which contained remarkably precise information about some 900 potential targets—an inordinately large research product for a group with such limited membership.

According to Sgt. McCree, the terrorist groups were able to exploit the intelligence resources of a number of far left Research Collectives, which he identified as (1) The North American Congress on Latin America (NACLA); (2) "Counterspy"; (3) the Bay Area Research Collective; (4) the several research collectives operated underground by the Weathermen, including the New Dawn Collective and the Jack Rabbit Collective; and (5) Resource One, a computerized operation in the Los Angeles area.

By way of illustrating his contention, Sgt. McCree quoted from the "Methodology Guide" put out by the North American Congress on Latin America. Talking about general biographical sources on establishment personalities, this Guide said:

The single most valuable source in all types of power structure research is "Who's Who in America" which contains a great deal of information on most of the people it lists, often to be used in close connection in order to find people who have recently died, or to check the quarry's interests.

Sgt. McCree noted that the selection of the word "quarry" clearly implies that the individual who was the subject of the information was somehow being hunted. The encouragement to seek out the biographies of "people who had died," he said, suggests the use of deceased persons' identification for the purpose of establishing false credentials for the extremist underground.

In the case of Resource One, Sgt. McCree affirmed that its research focused heavily on political figures, corporations, corporate executives, law enforcement people, and similar establishment categories, and this research was readily available to extremist and terrorist groups.

The testimony given by Sgt. McCree and the other enforcement experts on terrorism who testified at this hearing pointed to the strong probability that the so-called "research collectives", in addition to providing intelligence used by terrorist groups, also functioned as ideological and conceivably operational coordinators. The following exchange took place:

SENATOR THURMOND. You speak about solidarity among those various terrorist groups. Have you obtained any information that there is any central direction given to these various groups? Are they just operating, do you think, independently as revolutionary groups?

MR. MCCREE. I would say the research collectives are probably giving this direction—if there is what you would call a central direction or strategic command.

The Prairie Fire Organizing Committee, the New Dawn Collective, the Bay Area Research Collective, Resource One, the North American Congress on Latin America—collective organizations like these, and like the Jack Rabbit Collective, appear to be publishing documents proselytizing, suggesting if you will, methods of operational procedures and that sort of thing. I am referring to study or research groups commonly known as collectives.

MR. HANSEN. If I might interject along that line. As Sergeant McCree indicated, the Weather Underground has a great deal to do with direction, as far as some of these groups go, through their publications "Prairie Fire," "Osawatomie" and whatnot.

The theory is that many of the bombings perpetrated, say, by one group, the New World Liberation Front, is in fact many groups operating under an umbrella title. This is the

classic guerrilla cell structure. The titles are generic in nature.

* * * * *

Mr. SOURWINE. Do you know of any evidence of ideological and personal interlocks between the NACLA and Resource One, the Bay Area Research Project, and other terrorist organizations and individuals?

Mr. McCREE. Their own documentation and publications is the only thing I can use to establish any sort of interlocks. For example, Resource One admits in its own publication here that it's doing a common interest research project on the CIA with NACLA, Latin American Perspectives and Fifth Estate Counterspy. For that matter, Mr. Agee, who is on the staff of Counterspy himself, acknowledges the assistance of NACLA in getting research material. I would take him at his word for that. I don't have any independent verification of that, but Mr. Agee himself says that's the case in his book.

To further make reference to Resource One's newsletter, their computerized NACLA information would be available to, I quote:

"Other groups who currently don't have in-depth research libraries . . . Such groups might include radio stations, legal defense committees, and alternative news services . . . Eventually, one could find information, for example, about multinational corporations and their subsidiaries, agencies of city government, welfare procedures, local decisionmakers, housing or whatever, from any R/O terminal. In another NACLA project, the R/O computer is being used to process data on the Chilean corporate elite . . . The data includes the directors and principal stockholders of the 100 largest Chilean corporations, American subsidiaries and major banks and other financial institutions. The study should help reveal the interconnection within the corporate structure and help in understanding the American interest in and response to events in Chile over the past several years."

I would submit that this could easily be interpreted as an international target list.

Two central and complementary facts emerge from all this testimony. On the one hand, our law enforcement agencies operate under crippling intelligence restraints, while laws and regulations and the perceived requirements of these laws and regulations have combined to create a climate which has virtually made impossible the sharing of intelligence or meaningful cooperation against the terrorist threat. On the other hand, the various terrorist groups operate freely across state lines, sharing common intelligence resources that frequently operate in a *quasi* public manner and sometimes enjoying the benefits of coordinated action through their common connections with the research collectives.

Given such a completely unbalanced situation, it is not surprising that our domestic terrorist groups have, by and large, been able to operate without fear of apprehension or punishment.

What must be done

Clearly something must be done to restore the intelligence capabilities of our law enforcement community. If we do not do so, the opportunities for the terrorist fanatics in our midst will be limitless. In the course of his questioning of Chief Powell of the U.S. Capitol Police, Senator Thurmond posed the following question:

Suppose a group like the Hanafi Muslims had decided to make a surprise attack on the Senate Office Building instead of the B'Nai Brith and the D.C. Municipal Building. Without any warning, would you have been in a position to prevent them from seizing the building and taking all Senators in it hostage?

To this, Chief Powell replied:

We probably would have been able to prevent them from taking complete control, but there certainly would have been a loss of life and there probably would have been an open gun battle between police officers and this group. . . . I would suppose that equipped with sufficient firepower they would have been able to take charge of a given area.

On the need for a careful reexamination of the entire question of domestic intelligence, it would be appropriate to quote the wise words spoken by Dr. William Kintner, president of the Foreign Policy Research Institute of Philadelphia, and a former U.S. Ambassador, in his testimony before the Subcommittee on Internal Security, in June 1976:

I am all in favor of granting the widest possible freedom of expression to dissenting groups, including the most radical dissenters. But this does not mean that we must, in the name of the First Amendment, prohibit the gathering of intelligence about conspiratorial activities designed to overthrow our Government and destroy our freedoms, or to inflict mass violence or acts of terrorism on our communities which could take innocent lives. The line must be drawn somewhere. And to me it seems clear that the first purpose of the law in any free society must be protection of the community against violent and subversive minorities that seek to terrorize, intimidate, and slowly destroy the capacity of the Government.

Sgt. Arleigh McCree of the Los Angeles Police Department addressed the issue dramatically but much more concisely. He terminated his testimony with the words: "I would like to implore that we be given the tools back that we need to do our job."

CIVIL DISTURBANCES

During the 1960's, mass violence in our cities resulted in scores of deaths and in hundreds of millions of dollars worth of property damage. The violence generated in connection with the protest movement against the Vietnam War was clearly the work of various organized groups whose supporters, by and large, were ordinary American citizens opposed to the war, but whose leadership—as was documented by the House Internal Security Committee—came

primarily from the Communist Party, U.S.A., and from the Socialist Workers Party (Trotskyites).

There was at the time a tendency to assume that the orgy of burning and looting and killing that erupted in our major cities in the wake of the assassination of Martin Luther King was simply an expression of the accumulated grievances and the pentup indignation of the Nation's black minority. However, testimony taken by the Senate Permanent Subcommittee on Investigations and the book, "The Riotmakers," by Eugene Methvin, established beyond question that a broad spectrum of extremist groups was active in promoting and extending the extremely destructive riots that occurred during this period.

The damage done would have been much greater if our law enforcement authorities, during the 1960's, had been as completely deprived of intelligence capabilities as they are today. They were able to limit the damage and ultimately to bring the situation under control because, thanks to the use of informants and traditional methods of surveillance, they had knowledge of the organizations and personalities involved and some foreknowledge of their plans.

On June 18, 1976, the Subcommittee on Internal Security took testimony on "Threats to the Peaceful Observance of the Bicentennial." The witnesses were: Inspector George Fencl of the Philadelphia Police Department, Deputy Chief Robert L. Rabe of the Washington, D.C., Police Department, and former Ambassador William Kintner, at that time head of the Foreign Policy Research Institute of the University of Pennsylvania. There was great fear at the time of the hearing that the observance of the Bicentennial might be marred by violence and civil disturbances, promoted by various leftwing organizations and coalitions that were calling for protest demonstrations in both Washington and Philadelphia.

Inspector Fencl testified that "... the Prairie Fire Organizing Committee and other organizations had issued a call for mass demonstrations and disruptions of the July 4 activities in Philadelphia." He said that the so-called July 4 Coalition, in which the Prairie Fire Organizing Committee was involved, had called for "Four Days of Raising Hell in Philadelphia." This was a threat that had to be taken seriously—first because the Prairie Organizing Committee made no bones about being a public support apparatus for the Weather Underground, at that time the most active terrorist organization in the country; and second, because a number of the other participating organizations, most notably the Puerto Rican Socialist Party and the American Indian Movement, had a track record which definitely suggested a capacity for violence. Describing the discussion which took place at a July 4 Coalition meeting at the University of Pennsylvania on March 13 and 14, 1976, Inspector Fencl said that the speakers had urged that "attention should be focused on museums, statues, forts, and so forth, and physical action should be taken against them and that every time the rich celebrate, we should be there and be visible for the 4 days."

Deputy Chief Rabe spoke of his grave concern over the possibility of violence in the Nation's Capital over the Fourth of July weekend. He said that "there now appears to be solidarity between the various radical groups to unite under a single leadership such as the July 4 Coalition in Philadelphia." He also noted in his testimony that

"many aboveground groups have their more militant underground units which carry out the orders of the leaders, using more disruptive tactics, such as bombings and terrorist activities."

Chief Rabe and Inspector Fencel both made the point that they were operating under serious handicaps in their preparations for the July Fourth weekend because of their sadly reduced intelligence capabilities and the lack of intelligence in general. Chief Rabe noted that his department had received reports that there would be disturbances during the Bicentennial weekend "ranging from mass civil disobedience to multiple random bombings, all across the country, particularly in Washington, Philadelphia, Chicago, New York, and Los Angeles."

Inspector Fencel told the subcommittee that the Philadelphia Police Department was seriously concerned that it would not be able to control the situation with its own resources over the July Fourth weekend. He said that, based on the limited intelligence they had, Police Commissioner Joseph O'Neil and Mayor Frank Rizzo had already requested the President to send Federal troops to Philadelphia over the Bicentennial weekend to help police the estimated throng of over 1 million visitors, including two different radical coalitions, each planning its own march.

The Washington, D.C., Police Department had not asked for Federal troops. But Chief Rabe expressed his concern in these terms—

We, in law enforcement, would be negligent in our duties not to recognize that the potential and opportunity for violence exists and that the most critical period will occur over the Fourth of July weekend. Our task is twofold. First, we must insure that all preventative measures possible are taken in order to minimize the opportunity for any person or group to commit acts of violence; and, second, we must plan for an immediate and positive response to any threat of violence in order to prevent the commission of these acts.

Fortunately, there was no violence over the Bicentennial weekend. Despite the protest demonstrations, the hundreds of thousands of visitors to Washington and Philadelphia basked in the warmth of the Bicentennial spirit. By common consent—the spoilers notwithstanding—it was one of the most glorious weekends in the Nation's history. There is no intelligence available indicating why the various groups who had threatened violence apparently rethought their position and decided to abstain from violence. Conceivably, the public airing of some of their plans in the hearing helped to discourage them. Conceivably, they decided that any violence over the Bicentennial weekend would be politically counterproductive because it was certain to result in a sweeping condemnation by virtually the entire American people.

However, the dilemma confronted by the Philadelphia and Washington police at the time of the Bicentennial is bound to repeat itself on many occasions and in many cities so long as our law enforcement authorities remain deprived of meaningful intelligence capabilities.

It is a situation where our law enforcement authorities will frequently be damned if they do—and perhaps with equal frequency will be damned if they don't. If, in the absence of intelligence, they fear violence and seek to prevent it by a show of force, they open themselves up to criticism that they are "overreacting." If, on the other

hand, they underestimate the participants in a demonstration and violence gets out-of-hand because the number of officers on hand is inadequate, they are certain to be charged with failing in their responsibilities. Chief Powell, of the U.S. Capitol Police, admitted frankly that they might sometimes have more police officers on hand to deal with demonstrations than, on hindsight, turns out to be necessary. But then he noted that, at the time of the visit of the Shah of Iran (as was pointed out previously) due to lack of proper intelligence, the situation did get out-of-hand and the National Park Police were almost overrun by Iranian dissident students and their sympathizers. Having learned from this experience, the law enforcement authorities in the Nation's Capital mobilized sufficient force on the following day to maintain control of the situation.

This, however, is a very unsatisfactory way in which to have to operate. It is a virtual certainty that our law enforcement authorities at some point or points over the coming decade will again be called upon to deal with violent mass disturbances similar to the disturbances of the 1960's. They will have no strategic intelligence, because this has been largely destroyed, providing them with essential background information about extremist organizations which may become involved in the violence or about their ring leaders. Nor will they have any tactical intelligence about the immediate plans of these extremist elements, because tactical intelligence is clearly impossible without informants and without surveillance.

Such a combination of circumstances is a sure formula for catastrophe.

IX. CONSEQUENCES OF THE EROSION (II): THE WEAKENING OF THE WAR AGAINST DRUGS

Testimony submitted to the subcommittee also indicated that the erosion of law enforcement intelligence has had a significant adverse affect on our ability to cope with the army of drug traffickers who have made America the most drug-inundated country in the world today.

On this point, the testimony of Mr. Peter B. Bensinger, Administrator of the Drug Enforcement Administration (DEA) of the Department of Justice, was inconclusive and at points apparently contradictory. Some of Mr. Bensinger's statements suggested that DEA was able to operate almost in a "business as usual manner," despite the handicaps and restrictions which brought uniform complaints from all of the other enforcement witnesses called before the subcommittee.

Testifying on September 21, 1977, Mr. Bensinger replied in response to a question from Senator Thurmond:

Mr. Chairman, I am not sure I would share exactly your characterization that I believe the Drug Enforcement Administration is progressing quite nicely with respect to this legislation.

I do not think that it has had a documented adverse impact that I could represent to you in a statistical, factual, and representative manner, perhaps, as Mr. Knight.

* * * * *

I do not feel that I can represent to you that our information flow, as documented by the number of informants that we have active or by the type of intelligence that we share and exchange with Federal, State, and foreign agencies, has decreased. I just do not feel comfortable coming up and telling you something that I feel may be taking place if I am not in a position to prove it.

Mr. Bensinger's testimony was in strange disharmony with a DEA memorandum, dated August 30, 1977, dealing with the impact of the Freedom of Information and Privacy Acts on DEA investigations and intelligence collection. Written by Mr. Louis Bachrach, Chief of the International Intelligence Division, the memorandum—which was prepared in anticipation of the hearing before the Senate Subcommittee on Criminal Laws and Procedures—said the following:

In preparation for the anticipated hearings of the Senate Judiciary Committee's Subcommittee on Criminal Laws and Procedures regarding the above subject, the Office of Intelligence, in coordination with the Office of Enforcement, solicited field response on this matter using the attached cable (attachment A).

* * * * *

Generally, DEA field offices feel that enactment of the Freedom of Information and Privacy Acts has diminished DEA's ability to fulfill its mission, both in terms of conducting criminal investigations and collecting intelligence. Further, they are of the opinion that this negative effect is just beginning to manifest itself, largely as a result of a general public ignorance of all the laws' provisions.

The impact assessments made by DEA field offices generally contain the following three conclusions:

(1) Although thus far there has been a minimal increase in the reluctance of informants to cooperate with DEA, field offices predict that such cooperation will diminish substantially as potential informants and the general public become aware that the identity of informants can usually be determined through Freedom of Information inquiries. This will apply particularly in cases where potential informants are noninvolved witnesses and members of the business and professional communities whose cooperation would be entirely voluntary.

* * * * *

DEA field offices have conveyed the concern of local and State authorities concerning the sharing with DEA of local informants. These enforcement authorities are greatly concerned that DEA may not be able to safeguard the identity of their informants and are consequently increasingly reluctant to share these individuals with DEA or to identify the sources of any information they may provide.

(2) Another matter which has contributed to the negative effect on DEA of these Acts concerns the free exchange of information between DEA and local, State, and foreign enforcement agencies. In dealing with foreign governments, DEA foreign regions have detected a general concern about DEA's ability to safeguard the identity of foreign sources of information divulged to DEA in the course of joint investigations or in responses to domestic regions' requests for information. . . .

* * * * *

(3) Although no major DEA sources of information have yet been closed, there has been a noticeable constriction of information flowing to the agency from members of the private sector, e.g., phone companies, banks, hospitals, utility companies, hotels, pharmaceutical companies, and small private businesses. The amount of information previously provided on a voluntary basis has decreased markedly whereas information previously provided in response to simple requests can now often be obtained only upon service of an administrative or grand jury subpoena. Making this situation even more difficult, there has been an increased tendency on the part of businesses served with such a subpoena to immediately notify the affected customer that he or she is the subject of DEA investigation, thus compromising said investigation.

In closing, I would like to quote a particularly appropriate and generally representative sentiment expressed in Jerry Jenson's response to Attachment A for DEA's Los Angeles Regional Office:

"The real costs and effects of the FOI and Privacy Acts cannot be measured in terms of man-years or dollars, but by the increasing difficulty of collecting information and keeping our sources confidential."

This comment reflects both my own personal belief and that of the large majority of DEA field offices responding to our inquiry.

Mr. Eugene Rossides, former Assistant Secretary of the Treasury, expressed the conviction in his testimony that the war against drugs, in addition to suffering from the direct impact of the Freedom of Information Act and the Privacy Act, has also undergone serious attrition as a result of the breakdown of cooperation between the concerned Federal agencies, in particular the DEA and IRS. Mr. Rossides testified that he was primarily responsible for the short-lived Treasury and IRS Narcotics Trafficker Tax program, which he described as "one of the most successful law enforcement programs in our history." As a result of this program, he said, "over a very short period of time, 1,800 major dealers were identified and investigations started on most of them, along with 3,000 minor dealers." He attributed its success to "proper intelligence-gathering activities".

Mr. Rossides said that the program stressed the importance of going after the illegal profits of drug trafficking. "If a criminal case could be made," he said, "fine. If not, there was to be a full civil suit for taxes owed and civil penalties, if any."

Mr. Rossides described the Narcotics Trafficker Tax program in these words:

There were three aspects of the program: Target selection; IRS audit investigations; and prosecution or civil litigation.

The target selection process was designed to pool all the available information in this country from all Federal, State, and local law enforcement agencies as to who the major narcotics dealers were. There was no such data bank. There was very little cooperation among the agencies in exchange of information.

Guidelines were issued to insure adequacy and uniformity of response. We wanted the names of alleged major dealers but also details of their assets and standards of living so as to determine whether a tax audit would be warranted. Our aim was to take the profits out of the illegal narcotics trade.

Mr. Chairman, we got cooperation among agencies that had fought, jurisdictionwise, for years. Why? Because the tax function was not an overlap of jurisdiction. They could all validly cooperate with our program of identifying major dealers, and information with IRS and not in any way feel that they were giving up drug enforcement jurisdiction.

We set up field target selection committees throughout the country composed of Federal, State, and local law enforcement agencies for the purpose of giving us the advantages of a combined intelligence operation.

Information on each alleged major narcotics trafficker was pulled together. The field target selection committees would accept or reject potential targets based on information gathered by the various Federal, State, and local agencies.

Those selected would be sent to Washington for review by a Treasury target selection committee composed of representatives of IRS, Customs, and the Justice Department's BNDD.

* * * * *

Those selected by the Treasury target selection committee from field recommendations would be transmitted to IRS for a full-scale tax audit. It would be an IRS case run by IRS personnel and in accordance with all applicable agency procedures. If criminal action were warranted, IRS would refer the matter to the Department of Justice. Otherwise, civil action would be taken where appropriate.

In the judgment of Mr. Rossides, the success of this cooperative program was the prime reason for the downturn in heroin availability in 1972 and 1973. The program, however, was not to last long. On this point, Mr. Rossides recounted:

Unfortunately, in 1973 and 1974, after I had returned to private practice, the then-new Commissioner of IRS, who disagreed with the program, ended it despite clear congressional and executive policy and directives in favor of the program.

Without the revival of such a program, with a foundation based on intelligence gathering and the exchange of intelligence among Federal, State, and local law enforcement officials, we will not be able to reduce illegal drug operations in this country to manageable proportions.

Testimony taken by the subcommittee from other witnesses suggests, however, that the kind of interagency cooperation which Mr. Rossides stipulated as an essential condition for an effective war against drug traffickers is becoming increasingly more difficult, as a result of the cumulative effects of the Privacy Act on the free exchange of information between Government agencies. Indeed, IRS witnesses made it clear that as matters stand today they would not transmit to the appropriate Federal agencies information relating to the commission of nontax crimes, which their investigators had developed, or stumbled on, in the course of their tax examinations.

X. CONSEQUENCES OF THE EROSION (III): THE IMPACT ON CORPORATE AND PUBLIC SECURITY

The primary function of corporate security operations traditionally has been a preventive one. "Corporate security" is a concept that blankets virtually the whole of American society; the term embraces banks and insurance companies, manufacturing industries and utilities, trucking and railroads and shipping, hospitals and nursing homes.

The functions of corporate security are as diverse as the operations covered by the concept. Although it has other aspects, these functions can be divided into two basic categories, the first having to do with the protection of people—both employees and the general public—and the second having to do with the protection of corporate property and assets and information. Employees and the general public have to be protected against the possibility of terrorist acts, rapes, muggings, or other violent crimes. The corporations themselves must be protected against theft and fraud and embezzlement and penetration by organized crime and industrial and foreign espionage.

To cope with these manifold responsibilities, corporate security from its earliest days enjoyed a natural cooperative relationship with law enforcement and law enforcement intelligence. One of the most damaging effects of the widespread erosion of law enforcement intelligence has been the breakdown of their cooperative relationship. On the one hand, this has resulted in enormously enhanced problems for security directors and in a reduced ability to provide effective protection for people and property. On the other hand, it has adversely affected law enforcement by increasing its investigative burden while eroding the ready cooperation it used to enjoy with private security, in every area and at every level.

In attempting to assess the degree of damage, the subcommittee took the testimony of nine witnesses who are experts in the security problems confronted by various industries. The witnesses were provided by the American Society for Industrial Security (ASIS), which has 10,000 members in some 3,000 businesses and also includes security practitioners from governmental agencies and institutions.

Describing the scope of the private security problem, Mr. E. J. Criscuoli, executive director of ASIS, pointed out to the subcommittee that, according to a 1974 report, the annual cost of white-collar crime at that time had already passed the \$40 billion mark, while the cost of other crimes was estimated conservatively at \$50 billion annually.

There was virtual unanimity on the part of the witnesses from the security field that, because of the erosion of law enforcement intelligence and because of the direct impact on the private sector of the Privacy Act and parallel State legislation, the situation was becoming progressively worse.

On this point, Mr. Criscuoli testified:

Business and industry presently face the serious prospect of hiring individuals associated with organized crime, with histories of involvement in white-collar crime, or traditional

CONTINUED

1 OF 2

crimes such as arson and rape and numerous other modes of violent behavior. For instance, presently business and industry could easily find itself employing a felon as a computer operator or programmer, who in turn could steal valuable private and confidential data on members of the public and make such data available, for a price, to numerous criminal syndicates.

There is, at present, a growing network of criminal fences that specialize in the buying and selling of valuable confidential data, trade secrets, computer programs, and other valuable assets of American business and industry. Present legislation makes it difficult, if not impossible, to weed out criminal elements as potential employees.

I would also like to note, Mr. Chairman, that these criminal elements could easily make this valuable stolen data available to agents of foreign powers.

The present governmental red tape and legislative chaos that permeates this country also hampers the private security sector, making it difficult, if not impossible, for this sector to protect the rights and interests of the public-at-large.

The public, Mr. Chairman, is the ultimate victim of this growing erosion.

Among the points made by the security experts who testified were the following:

- Private security experts have little or no access to law enforcement intelligence that might help them to protect their corporations more effectively—first, because law enforcement agencies are hobbled by a growing body of statutory prohibitions, both Federal and State; and, second, because they have far less intelligence available to help them discharge their mandated responsibility.
- Second, what little intelligence law enforcement agencies have today, they do not feel free to exchange among themselves, as they previously used to do.
- Third, as matters stand today, the private security sector has little or no access to the intelligence on file with law enforcement agencies at the local, State or Federal level.
- Fourth, the private security sector is restricting the information it provides to law enforcement agencies, primarily because of its concern over the possibility of civil suits.
- Fifth, employers are now unable to get meaningful background information about applicants for employment. Hospital attendants cannot be effectively backgrounded prior to employment to make sure that they have not been convicted as rapists or arsonists; banks cannot check accountants before employing them to make certain that they are not hiring convicted embezzlers. They cannot screen their employees, as they used to be able to do, even when the job in question is a sensitive position that may involve the security of thousands of people or of millions of dollars of funds that ultimately belong to the public. Indeed, scores of thousands of people might be endangered if a nuclear facility employed a trained terrorist because of its inability to do background checks on employees.

• Sixth, many industries do not—or feel they cannot—provide information about a former employee to another industry, even where the employee in question has been dismissed for theft and indicted. They will pass on information about the theft only at the point where a conviction has been obtained.

Mr. Donald Duckworth, director of security for the Norton Co., a Fortune 500 manufacturer with plants in numerous countries, told the subcommittee that in preparation for his appearance as a witness, he had queried several officials of law enforcement agencies, ranging from local to Federal, with whom he maintained close personal liaison. All of them, he said, were unanimously agreed that their intelligence-gathering capabilities "had been drastically reduced—in some cases to the point of being nonexistent." The primary reason mentioned for this erosion was the enactment of the Freedom of Information Act and the Privacy Act. They were also agreed on the need for establishing "some institutionalized method for information transfer between the police community and the private sector due to the commonality of interest."

Mr. Duckworth told the following story about the stone wall he ran into when he tried to get information involving the possibility of terrorist action against the Norton Co.

Several months ago, a series of bombings occurred in Massachusetts. One, in particular, was directed against a major company, allegedly because of its business involvement in South Africa.

Since Norton Co. also has business interests in South Africa, it seemed logical that we also might be confronted with this type of incident.

When local, State, and Federal law enforcement agencies were questioned about the nature of the threat, the probability of additional bombings, the likelihood of us being a potential target, suspects' identities, description of perpetrators—in short, any information which would assist in an effective development and implementation of additional countermeasures—the same old refrain was heard: No information available, probably couldn't be released if it was available, no intelligence-gathering capability existing, intelligence unit disbanded, reduced, ineffective. In short, no information collected and none available.

A terrorist could have gone to work for us that day for the express purpose of infiltrating our organization, preparing intelligence data on the target—us—and assisting in the execution of the terrorist act.

In all probability, I would have never known it and the countermeasures which have been painstakingly thought out would have been totally ineffective, simply as a result of our being unable to develop accurate, credible information on the threat.

A number of the witnesses spoke about the difficult problem of defending their companies against organized crime, which, they said, has shown an increasing interest in using legitimate businesses as fronts and covers for illegal operations as well as to launder dirty money. Mr. Duckworth told the subcommittee of a recent incident

where the Norton Co. had been contemplating the utilization of a small concern as a national manufacturer's representative, until it discovered that one of the principals in this concern was on probation after having pleaded guilty to several charges of falsifying financial records and of illegally obtaining loans. The individual in question, although not justifying his actions, gave what appeared to be a plausible account suggesting some major extenuating circumstances. There was a suspicion, however, of organized crime involvement, based on certain aspects of the case. The Norton Security Department sought to obtain further information. Commenting on the outcome of this effort, Mr. Duckworth said:

When we attempted to move out of the open court records and further explore the situation through law enforcement agencies, we were stymied.

The same old refrain: No information available; if it was, not releasable.

I again ask the rhetorical question: How can you effectively prevent loss of assets from criminal activity if you are unable to determine that there is, in fact, criminal activity?

Mr. Robert B. Ross, director of security and safety for Trinity Lutheran Hospital, Kansas City, Mo., and chairman of the health care committee of ASIS, summed up the situation in these terms:

I can state with absolute certainty that law enforcement intelligence support for the private sector has ended almost completely, and we professionals in private industry who are trying to protect the public segment we come into contact with are severely hampered.

Mr. Criscuoli pointed out to the subcommittee that each crime prevented by private security reduces the burden on law enforcement by eliminating the need for another investigation, another apprehension, and another court case. Other witnesses dealt with the assistance that private security has been able to give law enforcement agencies when prevention broke down and a specific crime had to be investigated. Mr. Donald C. Drever, director of corporate security for the CNA Insurance Co. of Chicago, and chairman of the white-collar committee of ASIS, made the point that white-collar crime is complicated and takes a lot of time to investigate. Said Mr. Drever:

Whether it is my company or some other type of financial institution such as a bank or whatever it may be, each company knows its systems, knows its industry, and knows its terminology. An investigator would have to learn that.

So, I venture to say that, if most of private security which investigates criminal acts pulled out and left it up to law enforcement, that law enforcement would have to, as a general rule—other than some Federal and larger local entities—become much more sophisticated in investigations in certain areas. They would also have to have a lot more manpower.

Mr. Drever, however, then went on to state that, while his company has always cooperated with law enforcement, it is becoming difficult to continue to justify this policy when "cooperation is a one-way

street and there is no reciprocity when needed. We realize that this is not the fault of the law enforcement people when their hands are tied by the privacy laws."

Mr. Clifford E. Evans, director of security for First Federal Savings Association of Wisconsin, and chairman of the banking and finance committee of ASIS, also spoke about the growing reluctance in the private sector to pass information on to law enforcement authorities. Mr. Evans testified:

I would be happy to open up my investigative files to police departments. Many investigations do not come to fruition. The person terminates during the course of the investigation or there is not quite enough evidence to turn it over to police and to prosecution. But, yet, that information derived by the private sector during its preliminary investigation could be of value to law enforcement agencies.

In the past, we have been able to give them this type of information. Today, I know that I am extremely apprehensive, and I would basically not disclose any investigative information on a subject unless we actually had enough to give it over to the police for formal prosecution. There certainly are a lot of cases which never get that far. That is the kind of information that the police can use from the private sector, if only we felt free and uninhibited in giving it out.

For the breakdown in intelligence and the breakdown in communications between law enforcement and the private sector, the American people are paying a very heavy price—and the price may, indeed, turn out to be calamitous in the years to come.

On the one hand, because of the crippling of the security function, law enforcement becomes less effective even as it augments its manpower and its expenditures.

On the other hand, private security, deprived of the cooperative relationship it used to enjoy with law enforcement, is seeking to compensate for this handicap—like law enforcement—by adding manpower and security hardware. Mr. Criscuoli quoted the task force on private security of LEAA's National Advisory Committee on Criminal Justice Standards and Goals as saying:

There are more than 1 million people involved in private security in the United States. The private security industry is a multi-billion-dollar-a-year business, growing at a rate of 10 to 20 percent a year. In many large cities the number of private security personnel is twice the number of public law enforcement personnel.

The witnesses told the subcommittee that the security industry was rated as one of the three top growth industries in the Nation; that the ASIS over the past 5 years had essentially doubled its membership; and the security industry as a whole has grown to the \$6 to \$7 billion level.

The American public also foots the bill for the enormous increase in expenditures for private security because inevitably this becomes part of the cost of the products they buy.

On the subject of the continuing buildup of security personnel and hardware, the following exchange took place:

Mr. MARTIN. I'd like to ask this question: If we keep on adding to our security hardware every year—adding security guards at every industry and every place of business—isn't there a danger that as a result of this exaggerated regard for privacy, it will ultimately transform our country into a garrison society?

Mr. BAIRD. I'd like to answer that, Mr. Martin.

I think we're pretty close to being there right now.

Industry is very much concerned and so is the individual citizen. I, for example, have had my home burglarized twice. I personally have had to go out and spend approximately \$1,200 to put in an alarm system to protect my home and property.

The elderly in many of our cities live in great fear. They are attacked, robbed and beaten on the streets and even in their homes. It is not uncommon for senior citizens to equip their homes with all sorts of locks and devices to keep intruders out. Unfortunately, these fortresses are in fact their prisons.

Industry is also expending large sums on guard forces, fences, locks, alarms, et cetera, in their attempts to protect their property.

Yes; I think that we are rapidly approaching a garrison environment.

As a further illustration of the trend toward a garrison state, Mr. Henry Englisch, secretary for marine and aviation services of the Insurance Co. of North America, and chairman of the transportation and security committee of ASIS, described to the subcommittee the rigorous security procedures through which every truck driver approaching a terminal in the Port of New York area must pass.

The driver, he said, is stopped at the gate, his cargo compartment is searched, the front compartment is searched, and he is driven to a special holding area for incoming truckers. There the driver debarks from his truck and photographs are taken of both the driver and his documentation. He is then assigned to a waiting room until his truck is called to pick up its cargo. When he does pick up the cargo, the pickup has to be confirmed by the three separate signatures. As he leaves the gate, his truck is again opened and searched for the purpose of confirming that the cargo conforms to the bill of lading. The driver's compartment is again searched. And only after this exhaustive series of security procedures is the driver permitted to leave the terminal.

All of these security procedures, however, are not enough to prevent frequent instances of cargo theft. Mr. Englisch pointed out that a driver sometimes approaches the terminal

with an original bill of lading that was obtained by bribe, and, through his co-conspirators, he has timed his arrival to beat the actual pickup truck and make the ripoff, so to speak, in that fashion.

What this all adds up to, Mr. Englisch affirmed, is that additional hardware and security procedures are not adequate substitutes for a sound personnel program, supplied with adequate information.

THE "BAN" ON BACKGROUND CHECKS

The testimony provided by the witnesses from the security field converged on the theme that, while there is no formal ban on background checks for employees in the private sector, such a ban does exist for all practical purposes. This ban is the product, in the first instance, of the existing Federal privacy legislation, particularly the Fair Credit Reporting Act, the Privacy Act, the Freedom of Information Act, the so-called Buckley Amendment, and parallel legislation in many States. But perhaps equally important is the pervasive climate of fear and uncertainty, affecting private industry as well as law enforcement. There is fear because no one knows the answers to the question of what information can be released without violating the law or without opening the way to a civil suit, and there is widespread awareness of the tendency on the part of lower courts to rule in favor of personal privacy in all privacy-related cases.

The national security implications of this *de facto* ban on background checks was forcefully called to the attention of the subcommittee in early 1977 when it was looking into the problems posed to the Trans-Alaska Pipeline by the threat of terrorism and sabotage. Some 20,000 people—mostly from out-of-State—were involved in construction of the Trans-Alaska Pipeline, housed in a series of large construction camps of 1,000 to 1,500 workers. The pipeline's economic importance by any rational standard makes its security of national concern. Some of the control installations are so sensitive and compact that a single well-planned terrorist action could put the pipeline out of commission conceivably for months. Despite this, there was no backgrounding of employees. Mr. Robert Sundberg, chief of security for Alyeska, told the subcommittee that his company was not even attempting to obtain any background information about employees or applicants for employment "because it can't be done legally, and I would not advocate doing it illegally." [The caveat should probably be made that Mr. Sundberg, when he talked of "backgrounding", was talking in terms of effective backgrounding. The same caveat would hold true for the testimony of other witnesses. Backgrounding, per se, is not illegal, but statutory prohibitions make effective backgrounding impossible or at least prohibitively expensive.]

Mr. Sundberg was asked: "Suppose it came to your attention, despite these restrictions under which you operate, that an employee on a pipeline pump station or in some other critical segment of the pipeline had been involved in violent or terrorist activities, is there anything you could do about it?" The reply was that during the construction phase, even such knowledge would be insufficient to justify the dismissal of an individual so long as he was performing his job in a satisfactory manner. "Because of the freedom being enjoyed at this time," said Mr. Sundberg, "we may not, or Alyeska in all probability will not, be able to dismiss the individual for past activities." Mr. Sundberg made it clear that he was using the word "freedom" in quotation marks.

Witnesses in the series of hearings dealing with the erosion of law enforcement intelligence also testified about the practical impossibility of removing employees if adverse information came to the attention of their companies subsequent to employment.

Speaking about the informal but nonetheless effective ban on background checks, Mr. Henry Englisch on the basis of his experience in the field of cargo security, testified:

There has developed between industry and law enforcement and within industry itself . . . a general reluctance to even look for this information for the simple fear of placing yourself or your company in a liable position.

An individual can see, as can the company, the costs and time involved in this type of pursuit are totally unacceptable to an industry today.

As a result, you find that personnel officers and security officers will refrain from even attempting to obtain information on that basis, for the simple reason that they cannot use it.

* * * * *

I'm sure you're aware that you are no longer allowed to ask a person's age, marital status, or anything like that. The closest I've seen to being specific is an entry saying: Are you under 18 or over 40?

The inability to perform meaningful background checks even applies in the case of law enforcement agencies. Chief Powell of the U.S. Capitol Police told the subcommittee in his testimony:

Recently we had an occasion to investigate an applicant for our police force. We were confidentially alerted that we should take a look at this man's file. He had been a police officer in another area.

We sent one of our investigators to that location. He was not allowed to look at the applicant's personnel folder because they said that under the Privacy Act they could not allow us to look at his file.

I think that is probably a misinterpretation on their part of the law. But, nevertheless, we face that problem. We cannot order them to let us see the file of this former officer.

But it goes on and on.

* * * * *

It is a disservice to the applicant, it is a disservice to you not to be able to get qualified men or people you know would be loyal and you could depend on. It is a disservice to the people down there because, whether self-imposed or not, they feel compelled to work under this restriction and not disclose information that might be helpful.

Many of the witnesses underscored the dangers inflicted on the general public by the inability of private firms to control the hiring process. Charles Rice, professor of law at the University of Notre Dame Law School, told the subcommittee:

I do not think it needs to be said here how dangerous are the consequences, not only in terms of hiring people who are going to engage in theft, and larceny, and that sort of thing, but also in preventing infiltration of legitimate concerns by organized crime, and, preeminently, in preventing terrorism.

Here again, you are coming up against the disregard of the rights of other employees of these concerns who have a right, it seems to me, to be protected against having to associate in their working situation with employees who are bent on terrorism.

If I am an employee of any company, I think that concern owes me the duty to restrict the people it allows into a sensitive position who may thereby be put in a position to blow my head off by a terrorist act.

There seems to be a complete disregard of the faceless victims of these acts, again, in deference to a concentration of an exaggerated, absolutized, concept of the right of privacy.

Mr. Frank Carrington, in "The Defenseless Society,"—the study which he submitted as an exhibit at the hearing—presented a number of real-life horror stories dealing with the consequences of employment where background checks have been rendered impossible. One such case history dealt with a January, 1976 fire in a Chicago nursing home which killed 15 patients. "Police, suspecting arson," said Mr. Carrington, "checked the records of the employees of the nursing home, one of whom had been questioned in two previous suspicious fires but had not been charged or convicted for either. Arson investigators recognized her name, she was arrested and indicted on 15 counts of homicide."

Thus, in the excessive desire to protect the privacy of a nursing home employee by sealing law enforcement records against background checks by her employer, the lives of 15 innocent people were forfeited.

Other cases similar to this were cited by Mr. Ross in his testimony dealing with the problem of hospital security.

Mr. Carrington, in his testimony, also spoke of the dangers affecting every household because of the unavoidable need to permit third-party entries—for example, by utility repairmen. "If the telephone company hires a man to go into people's houses to fix telephones," said Mr. Carrington, "and that man is a convicted rapist, the telephone company cannot get that information. They issue the credential and you accept the credential in good faith and let the man in and he commits a crime, and you have another class of victim." This victim, he said was, in effect, a street crime victim, because of the inability of the telephone company to do background checks on its employees.

Professor Rice made the point that this situation constituted a violation of the privacy of the home, a fundamental right that has been strongly upheld by the Supreme Court in a series of decisions. Commenting on this contradiction between the consequences of the so-

called "privacy laws" and the law relating to the privacy of the home, Professor Rice said:

In this sort of situation, you rely on the telephone company or the post office, or whatever concern it is—the United Parcel Service—you rely on their screening their employees. When they, on the basis of that justified reliance, introduce into your home a person who is a threat to you, it seems to me not only trifling with your life, but also, if you want to talk about the right to privacy, overriding the right to privacy where it has been recognized—the privacy of your home, the right to be secure against intrusion into your home.

This is one of the areas where the right of privacy has been long recognized in the common law of tort—the right against intrusion.

The legal contradictions resulting from the privacy laws were also stressed by Mr. Carrington. Private companies, deprived of the ability to do background checks on their employees, clearly should not be held responsible, under any logical standard, for the actions of the employees they are obliged to hire under these blindfold conditions. In practice, however, they have been held legally responsible in a number of instances. Mr. Carrington related the real-life case of John Doe, who was hired as a deliveryman by a Montgomery County, Md., employer. The deliveryman was an ex-convict—a rapist on parole—but the employer had no way of knowing this. In a housing complex, related Mr. Carrington in "The Defenseless Society," the employee—

commits a crime of opportunity—another rape, and this time a murder. He is caught, convicted, and goes back to jail, this time for life.

The victim's husband sues John Doe's employer for compensatory and punitive damages, contending that the company was negligent in employing a man with that type of prior record. In 1975, under these facts, a Montgomery County, Md., jury awarded in excess of \$13 million against the employer and in favor of the husband of the rape-murder victim.

The near-total inability of private concerns to obtain from law enforcement sources even public record information relating to indictments and convictions has been compounded by the limitations, or perceived limitations, governing the release of employee information by former employers.

Mr. Lindsay Baird told the subcommittee that, as an independent computer consultant, he got around to visit many different companies in the course of his business. He said that, because of the fear of possible defamation action and the tendency of the courts to rule in favor of the plaintiffs, he found "a very severe reluctance on the part of the corporate personnel managers to make available to another company adverse information about an employee who has committed

some form of criminal act within that company." Mr. Baird testified further:

The rule—the unwritten rule—seems to be that companies will only divulge the date of employment, the job title or position, and the date of separation, and often nothing more.

A few companies I have been in would make an additional statement as to whether or not the employee is rehirable—and no more.

Most criminal activity in my area of specialization—data processing—based on that 1973 study, indicates that as many as 85 percent of the subjects were not brought before a bar of justice.

As a concrete instance, Mr. Baird told the story of a young man who attempted to sell his company's customer name and address list to competitors. Involved were 279,000 names—and the asking price was \$2.00 per name. The employee was apprehended, dismissed, and indicted. However, noted Mr. Baird, the "personnel policies of his former employer were to only confirm dates of employment, job title, scope of work, and date of termination." Mr. Baird said that he happened to be present in the personnel manager's office when a call was received from another firm which was considering hiring the dismissed employee. The prospective employer was given only the dates of employment and job description. When Mr. Baird asked why the caller was not advised that the employee was not subject to rehire, or that he was currently under indictment, he was told: "It's public information; it's corporate policy; and they did not want to become involved."

Mr. Henry Englisch, in his testimony, confirmed that a similar situation existed in the cargo transfer industry. The following exchange took place:

Mr. MARTIN. Suppose an employee is caught in the act of pilfering. He's arrested and indicted. At that point, could you provide such information to another company if he applied for employment in another company?

Mr. ENGLISH. Not until a conviction was obtained. We would say that the individual left our employment.

We could not say that the man is guilty of anything until he is found so guilty. In so doing, I open my company to a state of being liable for our actions.

Now he may be discharged, and he may accept this discharge or he may not. If he is discharged in the cargo area, quite frequently, the next day, he'll be working for another company because he is replaced by other private employment means. He may go through a local or whatever he works for.

But he may find himself an indicted person for a year or more before his case comes to trial and working in an area where there is similar access to cargo.

Mr. Donald Drever, of CNA Insurance Co., said that his own company "feels that you should not put your head in the sand and pass on an offending employee to the next unsuspecting company." In response to a question from Mr. Schultz, he said that his company

"will advise another company that we have discharged an employee because of criminal conviction or for good cause." He said, however, that "there are many legal ramifications concerning suits of defamation if this is not done properly." And he noted further that "many companies . . . would rather not provide this information because they either are afraid they are breaking the law, or they don't want to get involved. It is becoming so that most companies will not talk with another company and exchange this information."

In summarizing his presentation, Mr. Criscuoli concluded with these words:

In conclusion, let me pose to this subcommittee several questions:

One: If business and industry, hampered by its inability to screen prospective employees, were today to hire a mentally unstable individual who, in turn, would have access to dangerous and deadly chemicals, drugs, or even bacteria within a plant, might that person not wreak serious havoc on the public? Should such a person not be screened so that millions of our citizens can be protected?

Two: Terrorists have shown an uncanny ability to penetrate the highest echelons of Government. Could not these groups, well-disciplined and highly motivated, easily render a crippling blow to the very fabric of our society? Have they not done so in other countries? Is the American public not entitled to be protected?

Three: Because of an inability to screen prospective employees adequately, today's health care community finds it difficult, if not impossible, to protect its customer, the helpless patient, adequately. For example, attacks from rapists and other criminal elements employed by this growing industry have become too common in our hospitals. Is not the helpless patient entitled to protection?

Who pays the price? It is your constituents, Mr. Chairman, and our fellow-citizens. These are the ultimate victims.

THE "CLIMATE OF FEAR"

Professor Charles Rice of the Notre Law School questioned whether the requirements of the laws governing the release of employee information were as stringent as they were perceived to be by law enforcement agencies or by private employers. He agreed however that there was uncertainty about aspects of the law and he suggested that much could be gained by making the language more specific. "It seems to me," he said, "the least the Privacy Act should do is to recognize and give to people in their homes some kind of protection to prevent . . . possible invasion by people who are masquerading with credentials which no longer mean anything."

The role played by uncertainty, and the fear resulting from uncertainty, was stressed by a number of the witnesses.

Speaking about the reluctance of employers to prosecute employees whom they have had to dismiss for wrongdoing, Mr. Criscuoli told the subcommittee:

In the "legal jungle" that we have to operate in today, many corporations in assessing the amount of expenditure that they will have to incur in order to prepare a solid—if there is such a thing—case to take even to the prosecutor in order to get him to be reasonably willing to continue the prosecution, gets to the point where it is better to do nothing because, as you said, on the bottom line, it costs more to present this "impossible dream" of a solid case with assurance of conviction. If you ever lose it, you have had it. If you are a multi-billion-dollar corporation, and if you are picking on the poor employee, you start off with one strike against you before you even come up to bat.

Mr. Evans, of the First Federal Savings Association of Wisconsin, also spoke about the "prevailing climate of fear" in both law enforcement agencies and private companies. A lot of this, he said, has to do with the various laws that have been passed governing personnel and referencing operations and the fear of civil liabilities. There is a reluctance, as he put it, "to stick one's neck out". There is no law which compels companies to give out information—but their reasoning is that there may be a law that says they cannot. The result is that they play it safe rather than deciding to take a chance.

To illustrate this statement about the reticence commonly displayed by law enforcement agencies, Mr. Evans mentioned the case of a supervisor of a large branch office of a financial institution who was arrested and convicted of shoplifting. The local police did not provide this information to the employer. When the employer, despite this, found out about the shoplifting incident and asked the police why they had not automatically conveyed the information, "the police explained that they felt they would be in violation of 'some law'. No specific law was given and to my knowledge there is no particular law against this. However there is a prevailing climate of fear about this type of thing . . . basically they are afraid to do anything."

Mr. Evans also made the point that companies find it impossible to keep up with all of the various State laws and this acts as a further constraint whenever there is a request for an out-of-state reference check.

THE PROBLEM OF NONPROSECUTION

The problem is further complicated by the widespread tendency on the part of private business and private institutions to avoid prosecutions, especially of white collar crimes. It was Mr. Criscuoli's estimate that fully 80 percent of such crime is not prosecuted. Hospitals, the subcommittee was told, will frequently opt not to prosecute in the case of employees caught in the act of drug use or drug theft. Financial institutions, in the interest of avoiding adverse publicity, similarly steer clear of prosecuting cases of computer theft, even where large sums of money are involved.

Mr. Drever testified that the CNA Insurance Co. definitely does try to prosecute and cooperate with the proper authorities in the enforcement of the laws. But he said that his company was probably unique in this respect and he did not know how long they could keep it up.

Mr. Evans concurred with Mr. Drever's estimate that the general tendency today is to avoid prosecution because of the effort and costs and risks involved. He said that while the several companies represented at the witness table had "pretty vigorous policies" on investigations and on followthrough leading to prosecution:

I leave it to your imagination as to how many other companies throughout the Nation have considered prosecution to be a hopelessly expensive task with little rewards or gain, and who have just considered the crimes that occur in their firm as a cost of doing business. They wonder why they should bother on following through on prosecution.

Prosecution, it was pointed out, is further discouraged by the nominal sentences frequently handed down by the courts. Mr. Criscuoli posed the question: "If you just stop and realize that 1 out of 10 individuals convicted go to jail, where is the bottom line for pursuing an investigation?" As an example, he quoted a west coast case involving a \$1 million computer crime. The individual in question got a 3-year suspended sentence.

THE "RIP-OFF" SOCIETY

Mr. Lindsay Baird submitted as an exhibit an April 28, 1976 article from U.S. News & World Report entitled "Ten Days to Rip-Off Society". The article was in the form of a national survey based on the records of newspapers in some 16 cities over a 10-day period of time. It was a horrifying compendium of dishonest and fraudulent activities by citizens at every level, including doctors, lawyers, politicians and appointed officials. Commenting on this article, Mr. Baird said:

We have an attitude problem in our country where ripping-off the system is almost an accepted way of life today. This attitude creeps throughout our society.

Mr. Baird expressed the strong belief that when a situation is created that makes it easier for people to rip-off society, this in effect encourages them to rip-off society.

The testimony given by the various witnesses points to the conclusion that if America today has become a "rip-off" society, this is in large measure because of the weakening of the entire fabric of law enforcement.

When law enforcement intelligence is crippled in the many ways described by the subcommittee's witnesses; when there is a near-total freeze on the exchange of information between law enforcement and private security; when employers are stripped of the ability to check on the backgrounds of those they employ—with former employers as well as with law enforcement agencies; when hardened and even dangerous criminals can effectively leave behind their criminal records by the simple device of moving to another State or even another city; when the majority of employees who are caught in wrongdoing are not prosecuted because of public relations considerations or because of the fear that the prosecution might cost too much, might result in nothing, and might even boomerang in the form of a civil suit; and when there is no such thing as swift and just and

commensurate punishment for those who are found guilty by the courts—when you have a confluence of so many factors which make it easier for people to “rip-off” society, it is small wonder that America today is being described as a “rip-off” society.

For all of this the American people are today paying a very high price in terms of the quality of their personal lives as well as the quality of their society.

SPECIFIC PROBLEMS OF SECURITY IN VARIOUS INDUSTRIES

In the opening paragraphs of this section, the problems confronted by a major manufacturing concern, the Norton Co., were described in extensive references from the testimony of Mr. Donald Duckworth. Since the problems vary in certain ways from one corporate area to another, it might be useful at this point to round-out the summation of the testimony presented to the subcommittee by briefly recapitulating the statements of several of the witnesses from other areas.

Public utilities.—(Testimony of Phillip J. Cherico, director, Security and Safety, Power Authority of the State of New York.)

As director of Security and Safety for the Power Authority of the State of New York, Mr. Cherico has responsibility for three nuclear power facilities and four conventional power facilities. Mr. Cherico, in his testimony, underscored the growing concern over the problem of terrorism. The increase in terrorist activity, he said, is of concern to the entire public utility sector—and this concern is reflected in the criteria established by the U.S. Code of Regulations. He quoted the following passage from title 10, part 73.55 (a) as follows:

Licenseses shall establish and maintain an onsite physical protection system and security organization which will provide protection with high assurance against successful industrial sabotage by both of the following:

(1) a determined violent external assault, attack by stealth, or deceptive actions, of several persons with the following attributes, assistance and equipment: (i) Well trained (including military training and skills) and dedicated individuals, (ii) inside assistance which may include a knowledgeable individual who attempts to participate in both a passive role (e.g., provide information) and an active role (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack), (iii) suitable weapons, up to and including handheld automatic weapons, equipped with silencers and having effective longrange accuracy, (iv) hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or otherwise destroying the reactor integrity, and

(2) Internal threat of an insider, including an employee (in any position).

Mr. Cherico made the point that, while these requirements are imposed on the New York State Power Authority and other Federal licensees, in practice the privacy laws and the erosion of law enforcement intelligence have created a situation which make it impossible

for him to comply with the requirements of the U.S. Code of Regulations.

To comply with these regulations, the first requirement would be an effective personnel reliability program. This would involve a background investigation of all of those employees who have unrestricted access to the facility. This cannot be done when the intelligence and law enforcement records compiled by Federal, State and local agencies are for all practical purposes sealed.

Mr. Cherico noted that the U.S. Nuclear Regulatory Commission has proposed the establishment of a Federal clearance program for key employees of the nuclear powerplant industry. This program would be similar to the existing Department of Defense program for private industry. Mr. Cherico strongly endorsed the proposed clearance program, but he observed that while the "program may assist in establishing a personnel reliability program within nuclear powerplants, it does nothing for other types of power-generating facilities where terrorist activities could be focused."

The proposed plan, said Mr. Cherico, would do nothing to help them improve the security of their hydro facilities and their fossil fuel plants and "if you get into the gas area, the storage sites for liquid natural gas—these are the sites that could cause a tremendous amount of damage and harm to the public itself, and there is no clearance program scheduled for those activities."

The following exchange took place:

Mr. SCHULTZ. Is it your statement that there is no free exchange of information now relating to the very essential problem of the nuclear energy facilities; is that correct?

Mr. CHERICO. That is correct, sir.

Mr. SCHULTZ. Are you able to meet with the State, Federal, or local law enforcement authorities on any regular basis to even informally exchange information, or is this precluded?

Mr. CHERICO. We exchange information, that is, of the hard intelligence nature. For instance, let me give you an example. In May of 1976, just prior to the California referendum which was to do away with nuclear powerplants, or nuclear energy within the State of California, there was some information which was supplied to us by the Nuclear Regulatory Commission that in the 2 weeks preceding this scheduled referendum there were to be some demonstrations and possible activities against operating nuclear power plants.

We received that information, and we contacted the local and State agencies and asked them if they had that information, and they did not have it. So we passed that information on to them. So, what we have here is that one agency may have the information, but it is not disseminated to all of the agencies.

Mr. Cherico argued that, in order to protect nuclear and conventional powerplants against terrorists, there also had to be "an interchange of information regarding terrorist activities . . . between the appropriate law enforcement agency and the security division of the utilities involved."

Hospitals.—(Testimony of Robert B. Ross, Chairman, Health Care Committee, American Society for Industrial Security, and Director of Security and Safety, Trinity Lutheran Hospital, Kansas City, Missouri.)

Mr. Ross told the subcommittee that:

Hospitals, depending upon whose survey you read, are either the third or second largest industry in this country. They are big business, and the criminal element is aware that the industry started security programs about 5 to 10 years behind the rest of industry.

Mr. Ross submitted for the record a U.S. Department of Commerce study of hospital costs which stated: "It is rapidly becoming apparent that crime losses—primarily from theft and other business-related crime—are particularly responsible for the upward trends in costs of health care." Mr. Ross continued:

Preemployment screening is essential. Apparently the Commerce Department agrees with my thought which is that in order to reduce health care costs, we must reduce crime. The best way to reduce crime is to avoid hiring criminals. To do that, we need information during preemployment screening. The U.S. Government, via the Commerce Department, tells us that we must have that information. The U.S. Government, by law, tells us we can't have the information. [As noted previously the law does not actually prohibit backgrounding; it has simply made effective backgrounding impossible.]

Mr. Ross conceded frankly that, while the general public would not want hospitals to hire known rapists as orderlies or known drug addicts as janitors to do the daily cleanup in their pharmacies, hospitals, as matters stand today, simply have no effective way of pre-screening their employees. His testimony included 10 real-life case histories resulting from the inability of hospitals to perform background checks on applicants for employment. A few of these case histories are worth quoting for the purpose of bringing the problem to life:

In Houston, a male operating room nurse was slashed across the stomach and stabbed in the mid-back by a knife wielded by a housekeeping employee, following a verbal argument. During investigation, by the Houston Police Department, a record check revealed the subject had served six years in the State Penitentiary for murder. That 6-year time period had been falsified on the subject's employment application and personal and job references had been falsely reported by friends of the subject. Police records did not show out of town conviction on hiring check.

* * * * *

In Denver, a housekeeping employee was accused of making improper advances to another female employee. Investigation indicated the subject may be overly bold toward females but did not lead to a conclusion that the subject was dangerous. Two months later, he was arrested for the murder of

a nurse in a hospital office. Police investigation revealed the subject had a criminal history indicating violent behavior and had done time in Kansas. If the employment police check had revealed this information, more emphasis would have been placed upon the investigation of the subject's conduct, or he could have been assigned to a job where he didn't have ready contact with females. Either action may have saved the nurse's life.

* * * * *

A security officer in a hospital in New Jersey discovered and reported a large fire. Subsequent investigation revealed he set the fire. Additional investigation showed he had been terminated from another hospital for starting a fire there. No prosecution was involved, so without a conviction the information could not be passed on during the reference check. Subject's name was in police files as initiator of the first fire.

The inability to do background checks, is however, only part of the problem confronting hospital security directors. Speaking about other aspects of the problem, Mr. Ross said:

We now go to the hospital philosophy of no prosecution. Then we look at the criminal justice system and see that the preponderance of judges only slap the wrist of first-time offenders and put them right back on the street—if you can get a district attorney to try the case in the first place. And you can't completely fault the judges, either, because there really isn't any place to send many of these offenders anyway. So what happens to them? They are released to go seek employment at another hospital and continue to do their thing. When that hospital's personnel department sends for a reference, can our personnel department tell them "Jane Doe" was terminated for theft or "John Brown" was terminated for drug abuse? Not unless we want a healthy lawsuit against us. The current Federal law says we can't.

Even if I get authority from my administrators to prosecute, trial delays, continuances, et cetera, still permit this narcotics thief and user we have discharged to go to another hospital because they haven't come to trial yet and may not for 6 months. I still can't let the other hospital know, because the prosecutor may have decided to go the court route instead of grand jury indictment and without indictment or conviction, we cannot tell the next employer about the danger of hiring this ex-employee of ours. [The prohibition referred to by Mr. Ross is one enforced not by the law but by the fear of possible civil litigation.]

Mr. Ross, in concluding, repeated his plea that hospitals have restored to them the ability to obtain background information about employees, to help them reduce hospital crime and reduce hospital costs. His prepared presentation terminated with the warning words: "The next victim of a hospital crime may be you."

The cargo transfer industry.—(Testimony of Henry Englisch, secretary, Marine and Aviation Services, Insurance Co. of North America,

Philadelphia, Pa., and chairman of the Transportation and Security Committee of the American Society for Industrial Security.)

Cargo theft according to the most recent estimates, costs American industry tens of millions of dollars annually. The prevention and investigation of cargo theft is an enormously complicated business. Mr. English noted that:

A considerable portion of cargo theft is a result of collusive effort between employees of transportation companies and between those employees and employees of cargo shippers and receivers. Of course, and not to be excluded, are employees of peripheral industries, such as insurance companies and agents, cargo brokers and banks—all of whom have access to cargo, insurance, and credit documents, which in turn can be used for hijacking, theft, and pilferage purposes.

Mr. English further told the subcommittee:

When one realizes that a considerable amount of what could be termed sensitive cargo is constantly in transit in all transport modes, it becomes evident that, with limited security capabilities, the purposes of terrorist groups may well be served.

Nuclear fuels and explosives are examples of cargoes that could be seized and used for terrorist activity or extortion purposes.

Just a few weeks ago we had a situation in the State of Florida in which a pesticide was introduced into a municipal water system, with fortunately no deaths involved to my knowledge, but a situation of great consequences.

The ability to obtain quantities necessary for this type of terrorist and extortion activity usually rests in the Transportation Act—where due to lack of security a similar material might be obtained from a rail car, a platform, or through collusion with an employee of the shipping and transportation company.

All transport modes—rail, motor, air, and marine—are subject to the cargo theft problem. But even greater hazards exist—those which include disruption or destruction of transportation facilities—which could be perpetrated for extortion or terrorist purposes or to interdict defensive efforts on the part of our military forces.

Employees of the transport industry are frequently entrusted with the safety and security of literally hundreds of lives and major dollar values at any given time.

I submit that this special trust is of a magnitude and gravity rarely matched in other industries. Accordingly, the confidence placed in these employees by the public must be based on the highest order of proven reliance and competence.

These facts, said Mr. English, made it essential to transportation industry employers that they have access to criminal record information on prospective employees. But they do not.

Because cargo in transit can be simultaneously local, interstate and international in nature, and because employee collusion can extend across city, State and national boundaries, said Mr. English,

"criminal information intelligence from many jurisdictional sources is vital to the effective control of cargo theft."

Speaking in broader terms about the security problem in general, Mr. Englisch said that "a free, rapid, and continuing exchange of criminal intelligence between law enforcement agencies at all jurisdictions—local, State, national and international—is crucial to the safety and security of the people of the United States of America."

But this requirement for a viable cargo security program is also something beyond the reach of industry security specialists because of the freeze on the sharing of intelligence within the national law enforcement community and between the law enforcement community and private industry.

The sad state to which the sharing of intelligence relating to cargo security has been reduced was the subject of the following frank commentary by Mr. William E. Williams, Deputy Commissioner of the U.S. Customs Service, in response to a written question:

Question. What effect does the Privacy Act have on the exchange of information between private industrial security services and U.S. Customs as regards cargo security?

Answer. The Privacy Act acts as a deterrent in effective law enforcement in connection with imported and exported merchandise. As the Privacy Act prohibits the Customs Service from releasing information including intelligence on suspected violations to private security services, there is a loss of coordination and a diminution of the united front against cargo theft, pilferage and fraud which inevitably results in valuable losses to importers, exporters, private citizens and private enterprise. Situations exist in Houston, Miami, New York, and other metropolitan areas which reflect this problem. In Philadelphia, for example, the Office of Investigations has information and evidence of many cases of cargo theft, yet is prohibited by the Privacy Act from providing data to the Philadelphia Marine Trade Association (PMTA), who by contract with local unions have agreed to suspend union members apprehended in pilferage or cargo theft situations.

Although the PMTA is cooperating with the U.S. Customs Service, it represents a one-way of information. Customs takes intelligence of suspect activity from the PMTA, yet cannot reciprocate.

The same situation applies to railroad companies throughout the Nation. ConRail, Philadelphia cooperates with U.S. Customs in reporting cargo thefts and pilferage yet the Customs service is prohibited from providing information to ConRail's investigators.

In New York and other ports on the east coast, investigations have revealed some African nationals legally exporting their private vehicles. The Customs service later learned from the NATB (National Auto Theft Bureau) that insurance claims have subsequently been filed in claim of stolen vehicles. The NATB then requests information from Customs which may show the vehicle having been exported; however, the Privacy Act prevents the release of such information to private agencies.

These are but a few examples citing situations which require a freer exchange of information on criminal activity with the private sector.

The insurance industry.—(Testimony of Donald C. Drever, National Chairman of White Collar Crime Committee, American Society for Industrial Security, and Director of Corporate Security, CNA Insurance Company.)

In opening his statement, Mr. Drever said that the question of the affordability of insurance was intimately linked to the problem of privacy legislation and the erosion of law enforcement intelligence. Mr. Drever continued:

. . . It is not an emerging problem, it is here now and it is acute.

* * * * *

The insurance industry sells a promise—a promise to pay when it is needed. We have an obligation to pay what we owe—but only what we owe—not more.

However, recent and potential legislation concerning privacy issues will make affordability all the more acute. I believe that the following will show how affordability and privacy issues are linked together.

His testimony stressed the fact that every fraudulent insurance claim paid by American insurance companies and every payment for fire losses resulting from arson and every loss resulting from dishonest activities by employees had to be passed on to the insurance-buying public in the form of increased premium rates.

Mr. Drever presented a number of case histories from the files of American insurance companies to illustrate his point. One case history pertained to a 1976 accident—a seemingly routine incident involving a rear-end collision between two cars. The investigation of this one incident, however, revealed that it was part of a conspiracy a number of years old to defraud insurance companies, and that a total of about 260 men and women in Los Angeles and Orange Counties, Calif., were involved.

In investigating the 1976 accident, a few facts emerged which automatically pointed to the need for further inquiry. The family in question had been driving a 1968 Mustang at the time of the accident. On their second evening in San Francisco, their car was rear ended. The husband and wife immediately returned to Los Angeles and entered the hospital, where their bills quickly ran up to the \$5,000 level.

The investigators discovered that in late 1975 the couple in question had purchased a new Mercedes Benz on a short-term contract on which they were paying \$772 a month. In addition, they purchased a lot of jewelry and furniture during the same period. Their purchases during late 1975 committed them to monthly payments of \$3,900—all of which was backed up with credit disability insurance. The driver of the car which rear ended the Mustang was from Vancouver, British Columbia. But when the investigators probed a bit further, they discovered he was related to the claimants.

The family in question, noted Mr. Drever, was not only covered by Blue Cross and Blue Shield but by nine of the most generous medical policies they could get. In addition, they had each acquired

14 short-term accident policies, each of which was good for \$5,000 in medical hospital expenses resulting from accidents.

Commenting on the scale of the fraud involved, Mr. Drever said:

The potential profit for this attempted fraud on medical reimbursements alone would have resulted in \$230,000. The credit and disability insurance would have added much more.

The Los Angeles district attorney took this case and I understand his investigators obtained an admission from the couple that they had taken over \$440,000 out of the insurance industry in 1974 and 1975. This is larger than the profits of many companies.

Mr. Drever submitted for the record an article from the September 17, 1977, National Underwriter which discussed the conspiracy of which the above incident was a product. The article quoted California authorities as estimating that separate groups of Hungarian immigrants and Arab students were bilking insurance companies to the tune of about \$400 million a year.

Mr. Drever discussed the problems confronting insurance companies when they begin to have suspicions about claims submitted to them, especially the problem stemming from the reticence or the inability of the law enforcement agencies to share information with them:

Once we have assembled the facts, we are faced with several alternatives. We can pay, decline, and face a possible legal action, initiate a declaratory judgment or refer the case to the authorities for prosecution. In some States these alternatives can be very dangerous—especially, with the ever-present specter of enormous punitive damages, if we fail to sustain our refusal to pay.

If we choose the alternatives of referring the matter for prosecution, the law enforcement agency will normally ask us to discontinue further efforts so they may conduct their own investigation. They will also usually request that we do not pay the claim.

During their investigation we may be getting considerable pressure and the threat of legal action if we don't pay. At this point, we try to determine the status of the possible prosecution, but the law enforcement agency cannot furnish any information. Cases like this deserve prosecution. We do our best to cooperate, but we can only gamble so far on how much to cooperate without exposing our company to an unacceptable monetary risk.

The second example of an area for concern is murder-for-insurance. . . .

* * * * *

A good example of this involved a death claim last year of \$60,000 in a Chicago suburb. Our adjuster, during a thorough investigation suspected that the beneficiary had murdered her husband. He went to the local police department but could not obtain any information. Having stalled for some time and still not getting any response from the police, he paid the claim. A very short time later, the wife was jailed

for murder and later convicted. Result—the wife was in jail, and two small children are wards of the State, the \$60,000 having been immediately squandered away.

Had the police given us some indication of the possible indictment, the \$60,000 would have most likely gone to the children. We realize that their hands are officially tied, but there are times when we ponder the possibilities of an injustice if these bonds are too tight.

At the present time we are investigating a large potential medical and hospitalization insurance fraud ring in a mid-western city that may include up to 110 individuals. A Federal agency had some information concerning several members of the ring. They, however, were unable to advise us of the situation and we paid numerous claims involving thousands of dollars before learning of the possible fraud. I can't blame the agency for not advising us because of the privacy considerations, but who loses in the long run? The consumer, through increased costs.

Another very bad situation arises when you cooperate with the authorities, but they fail in their efforts to get a conviction. Recently, several companies provided testimony and documents to a grand jury. This was done at the request of the local law enforcement authority and they even acted by virtue of a subpoena.

Unfortunately, the local district attorney failed to sustain the criminal charges and they are now faced with a \$10 million damage case, alleging collusion with the police to damage the person's reputation, causing him untold mental anguish, and four other nebulous allegations. They gave the law enforcement agency full and wholehearted cooperation when it was needed. Now, when the companies need to conduct some dialog with them, they find the doors are closed. The companies will most likely defend themselves successfully, but it will be more difficult and costly because of the inability of law enforcement to provide information. As a result, this increased expense is paid by the consumer.

While preparing for my appearance here today, I talked with Mr. Frederick G. Stewart, deputy district attorney, Major Fraud Division, Los Angeles District Attorney's Office. Los Angeles is one of the insurance fraud capitals of the country. Mr. Stewart advised that he has specialized in the investigation and prosecution of insurance fraud rings for the last 2 years.

According to him, most insurance companies in California are frightened to cooperate because of bad faith lawsuits, the Fair Credit Reporting Act, and the Privacy Act.

Mr. SCHULTZ. Are these State statutes that you are talking about?

Mr. DREYER. He is referring to both State and Federal—

Mr. SCHULTZ. Thank you.

Mr. DREYER.—and the general confusion that exists because of them. He advised that he cannot file a case until he has documents and he cannot get the documents

because he is unable to get a subpoena until he has a case. As Mr. Stewart aptly puts it—a Catch 22.

In the case of arson losses, Mr. Drever pointed out that in 1975 these accounted for 37 percent of all fire losses or \$1.3 billion—this, according to the American Insurance Association.

The enormous cost of arson, needless to say, becomes part of the insurance premiums paid by law abiding citizens.

Mr. Drever terminated his testimony, in the manner of other witnesses from the security field, with a plea for an effective relationship between the law enforcement community and private industry in the interest of crime prevention:

An area where private industry needs to relate to law enforcement agencies is in new employee investigation. It is becoming increasingly difficult to determine the background of a potential employee. Companies are fearful of divulging information about past employees to other companies or law enforcement agencies. We cannot check law enforcement criminal history records for convictions.

And to complicate matters, many agencies are fearful of divulging information to other agencies. Where does this leave private industry? We have a real and legitimate need to know if criminally inclined individuals are attempting to work for us. I do not feel that an individual's right to privacy is mutually exclusive of a company's right to protect its employees and assets by trying to anticipate and prevent crime. There must be a way to protect the individual's privacy without crippling private industry's ability to complete a background check on potential employees for sensitive positions.

The Privacy Act of 1974 has all but sealed criminal history records. However, industry has a legitimate need for certain criminal information. In the past, criminal history records were inaccurate at times, and the release of such nonfactual information can and does cause harm. However, would it not be better to require criminal agencies to maintain accurate records of offenders as opposed to severely restricted access to an individual's criminal records, and, therefore, virtually hide it, all in the name of privacy?

Banking.—(Testimony of Clifford E. Evans, chairman, Banking and Finance Committee, American Society for Industrial Security, and Director of Security, First Savings Association of Wisconsin.)

"Financial institutions," Mr. Evans told the subcommittee, "will probably always be especially choice targets for crime since, as the infamous Willie Sutton once said: 'That's where the money is.' Because they are choice targets for crime, financial institutions have been especially hard hit by the erosion of law enforcement intelligence."

Depositors do not lose the funds they have in a financial institution as a result of bank robberies, embezzlement or fraud. It is the consumer, or depositor, who must pay for these losses in the form of higher loan rates—and he must also pay for the considerable cost of increased insurance and security measures.

On the subject of insurance, Mr. Evans noted—

. . . Many financial institutions cannot secure a fidelity bond for their employees due to the great increase in embezzlements, both computer and noncomputer. Since computer related embezzlements have gone into the millions of dollars, these financial institutions could conceivably experience total collapse as a result of a major embezzlement. The problem is becoming greater as insurance companies leave the blanket bond market.

Speaking about the damage done by the freeze on the sharing of information, both within the banking community and between the banking community and law enforcement agencies, Mr. Evans said:

Financial institution security executives have traditionally enjoyed a good rapport with law enforcement and previously they exchanged information with minimal restrictions. This has all changed now in that the police are very apprehensive about distributing intelligence information, and the financial institutions have been forced to shut off all information they could supply to the police, due to recent legislation and regulation.

The problem is even more acute in the exchange of information between companies regarding employee reference checks. Most companies will not disclose that an employee was terminated due to the commission of an illegal act, unless the employee is eventually convicted in court. Many companies will not even disclose a conviction.

An example is appropriate: Some years back First Federal terminated an employee who was arrested for stealing and cashing company checks. This employee sought work at another company, and when they called for a reference First Federal did not indicate the arrest since the person was still in the process of being convicted. This person was employed by the other company, placed in a position of trust, and promptly embezzled a large amount of money.

In discussing what could be done to improve the security of banks and other financial institutions, Mr. Evans stressed that "effective prevention can only be achieved through proper background investigations and internal control measures applied to employees who occupy positions of trust." In contradiction of this basic requirement, however, was the fact that "the erosion of law enforcement intelligence has severely hampered our efforts at performing background investigations on even our most critical employees."

Mr. Evans said further:

Intelligence information is sorely needed in the area of external crimes against financial institutions, specifically concerning check fraud and customer swindles. Check fraud professionals will usually enter a city and hit many financial institutions for 5 to 10 days and then move on to other cities. Knowledge of a forger's method of operation is essential for financial institutions to help in stopping the crime. Many law enforcement agencies will no longer supply the necessary

intelligence information, and, as a result, the check fraud artist's job is much easier.

* * * * *

Gentlemen, I do not appear before you to plead for law enforcement powers to be given to private security, for I believe that security is a business management function and not a police operation. I do believe, however, that private security is in need of law enforcement intelligence in order to effectively prevent crimes and losses from occurring. I realize that indiscriminate dissemination of intelligence information is reminiscent of a police state, and controls are needed to protect and preserve a free society. Given these controls and safeguards, I am convinced that the collection and dissemination of law enforcement intelligence information will not erode our free society but will serve to protect the citizenry.

Computer systems.—(Testimony of Lindsay L. Baird, Jr., Independent Security Consultant, and National Chairman of the Computer Security Committee, American Society for Industrial Security.)

In establishing his personal background, Mr. Baird told the subcommittee that his concerns, as a specialist in computer security, involve "the protection of computing systems from accidental, malicious, criminal, or unauthorized manipulation of systems, files, and data."

He estimated that at the time of his testimony (September, 1977) there were more than 680,000 computing systems in operation in the United States. He said that both industry and Government are becoming more and more dependent on computing systems for their day-to-day activity. While the Department of Commerce has estimated that losses from computer fraud exceed \$100 million per year, it was Mr. Baird's estimate, based on information developed by various studies, that the actual losses for the year 1977 would approximate \$1.5 billion.

In discussing the problems of computer security, Mr. Baird told the subcommittee:

The greatest vulnerabilities to the security of assets and sensitive information resident on computing systems are people.

The most secure physical environment offers little protection against dishonest, deranged, or disgruntled employees. The only measures by which an individual can be evaluated are past and current performance in education, business and society.

The Fair Credit Reporting Act and the Privacy Act of 1974 have impacted on our ability to determine the reliability of data processing employees, as well as all others, that fill positions of trust.

The Privacy Act of 1974 has all but sealed criminal records; however, industry has a legitimate and pressing need for selected criminal history information.

For a variety of reasons, noted Mr. Baird, industry is generally reluctant to report computer crimes to law enforcement agencies. This reluctance was generally justified on grounds of embarrassment, loss of public image, and the potential for a stockholder's suit. Inevitably,

however, computer manufacturers have had to give some consideration to the problem. In 1974, said Mr. Baird, he cochaired a seminar on computer security with the representative of a computer manufacturer. He made the following notes on his cochairman's presentation:

One, a study pertaining to dishonest employees in a data processing environment was conducted in 1973.

Two, between 20 and 30 events of dishonest activity were reported each month during this year-long study.

Three, the average per-event loss approximated \$674,000.

Four, 85 percent of the subjects identified in this study were not prosecuted.

Five, only one in five of the subjects referred to the courts received a sentence imposing confinement.

Six, the odds of a person going to jail are 1 in 33.

While he had not been able to confirm his notes with his cochairman, observed Mr. Baird, he had "every reason to believe that they are correct."

Mr. Baird also referred to the findings of a 1973 study on computer abuse by Don B. Parker of the Stanford Research Institute. The Parker study reported on 148 incidents of computer abuse, occurring between 1964 and 1973. Parker was able to obtain dollar loss data for only 65 of these cases. The total losses were \$90,514,000, which equates to an average loss of \$1,392,000 per computer crime.

In a followup study reported on by the February 23, 1976 edition of Crime Control Digest, Mr. Parker said that he had been able to interview 17 computer fraud perpetrators. Eight of these cases involved financial gain ranging from \$1,400,000 to \$1,500,000. Half of these cases involved collusion. Eleven of the 17 computer criminals he had interviewed held positions of trust.

The thrust of Mr. Baird's testimony was that what we have seen so far may only be the beginning—that there may be much worse to come. He noted that when Mr. Bullock, Chief of the Illinois Bureau of Investigation, was asked by U.S. News & World Report: "What's the next field for the organized criminal to conquer?" Mr. Bullock replied:

We know from our sources that figures in organized crime have expressed great interest in moving into computer fraud. They are taking a very, very strong look at it and they are prepared to move promptly. Someday we are going to read about one hell of a heist.

It is not merely money and company and Government assets that are at stake. The Nation's numerous computer systems, in addition to controlling fund deposits and transfers running into hundreds of billions of dollars, are also the custodians of much sensitive personal information and of precious commercial and technological data. These information systems can also be penetrated for dishonest or criminal purposes by those who are skilled in computer fraud.

A report on computer security in Federal programs issued by the Senate Committee on Governmental Operations in February, 1977, noted Mr. Baird, recommended (1) that computing systems which distribute funds and/or process highly private or economically valu-

able data be classified "critical sensitive" to help protect them from criminal abuse or manipulation of data; and (2) a tightening of personnel security practices to make sure that only trustworthy persons are employed in these sensitive positions. Commenting on these recommendations, Mr. Baird observed that, while the Federal Government has the statutory authority and resources to initiate an effective personnel screening program, "we in the private sector are not that fortunate, as criminal records, criminal intelligence, accurate investigative consumer reports, factual prior employment history, et cetera, are either not authorized for release or are not readily available."

Mr. Baird also called the subcommittee's attention to an article in the May, 1977 issue of Computer Security, captioned "You May Have to Hire Alcoholics or Drug Addicts in the Data Center Unless . . ." The article was inspired by a HEW rule banning job discrimination against the handicapped and by a more recent ruling by Attorney General Bell that the definition of "handicapped" includes alcoholics and drug addicts. On this matter, Mr. Baird commented bitterly:

. . . Must we then have alcoholics and drug addicts working in critical sensitive data processing positions that involve the distribution of funds and highly private or economically valuable data?

* * * * *

The Congress and the courts have been overly concerned with protecting the rights of the misfits in our society. They now have more rights and privileges than honest, law abiding citizens. It is about time someone started restoring the rights of both good citizens and industry to be safe and secure in their homes and businesses.

It was, however, the possibility of terrorist penetration of our computer systems that most disturbed Mr. Baird. On this subject he said:

The total loss of computer power for a period of 3 to 5 days can reasonably be expected to have catastrophic impact upon many companies. The severity of any interruption in the availability of this business tool increases at unbelievable rates the longer systems are disabled or unavailable for normal operations.

It is my firm belief that we will witness within a relatively short time an attempt by an activist group to achieve their ends, whatever they may be, by either holding a corporate computing system hostage or destroying a critical subset of a system with threats of disabling other components.

Italy within the past 12 or 13 months has been subjected to 10 attacks against corporate and Government computer centers by armed terrorist groups.

A front page article in Computerworld, August 29, 1977, provides some insight on how a small dedicated group of Communists can disrupt vital processing and cause millions of dollars in damage.

These problems may be associated with Europe today; however, I fear that radical groups may attempt to hold either a major corporation or Government data center for political or monetary ransom.

Witnesses before this subcommittee have identified a few of the radical groups and the thrust of their movements. Are we to let them, in the name of privacy, fair credit reporting, equal employment rights according to the newly defined "handicapped," and so forth—allow these groups to operate without surveillance in our democratic society?

There may have been abuses on the part of law enforcement and other intelligence-gathering agencies in the past. However, today they are almost totally ineffective due to the operational and administrative constraints Federal, State, and local legislative bodies have placed upon them.

Imagine what the consequence might be if a radical group occupied the Social Security Administration's (SSA) computer center a few days before the monthly checks to millions of Americans were produced.

A threat to destroy the 30-odd computers located in the SSA main data center alone will create sufficient fear in the hearts of man, HEW officials, the legislature, and the American people that the Government would most likely negotiate.

The results, undoubtedly, would be a victory for the terrorists and a resounding defeat for our system of Government.

THE NEED FOR BALANCE: A FEW RECOMMENDATIONS

All of the witnesses appealed for a more rational balance between the right of privacy and the requirements of law enforcement and personal and corporate security.

Mr. Criscuoli, speaking for ASIS, said in his testimony:

The right of privacy, supported and cherished by all of us, must be balanced within the legal and ethical framework with the rudimentary need of every society to protect itself against those who threaten its very survival.

Commenting on Mr. Criscuoli's testimony, Senator Strom Thurmond who presided, observed:

The thrust of your argument, as I understand it, is that in recent years the situation has gotten off balance so that today the entire emphasis is on the protection of privacy. As a result of this, not only has our society endangered itself, but we have placed a heavy cost on our own citizens. In the case of terrorism, we have even placed our lives in deadly danger—more so than would be the case if we had a better balance between privacy and the requirements of law enforcement.

Mr. Criscuoli confirmed that this was an accurate summation of his position.

The plea for a better balance between privacy and public security was reiterated in these terms by Mr. Donald Drever, of CNA Insurance Co.:

Legislation should not be passed that assists and hides fraud. CNA always has respected and supported the individual's right to privacy. We must question, though, the wisdom of any legislation which overly protects this right—to the point that it facilitates fraud or otherwise interferes with or prevents the conduct of legitimate business. Further, we wonder if the consumer will pay the increased costs that may result from present and future privacy legislation.

* * * * *

It seems illogical with the rising crime rate, especially for white collar crimes, and the inability of traditional methods to deal with it, that the private sector is severely restricted in taking actions designed to protect its assets and prevent crime.

Mr. Lindsay Baird, in addressing the need for better balance, told the subcommittee:

Life, liberty, and the pursuit of happiness are the concerns of all of us. However, we must have realistic and prudent measures by which we can collect and exchange meaningful and factual information about those individuals and groups that may intend to commit crimes and/or attempt to forcefully change our form of Government against the will of the majority.

The stockholders of companies, for example, are the losers, as is the consuming public. We pay for these crimes in the form of a tax—a rather hideous tax, called increased price of goods and services.

Several of the witnesses offered specific recommendations for improving the situation.

Mr. Cherico, of the New York State Power Authority, concluded his presentation with a strong plea for free dialog with the law enforcement agencies. He testified:

. . . I strongly believe that it is essential that we in the private security sector involved in the protection of nuclear power plants, their peripheral fuel cycle facilities, and other power-generating facilities, have the ability to have a free dialog and exchange with intelligence agencies, not only to meet the criteria already established by the U.S. Nuclear Regulatory Commission, but also to provide a sound and effective security program for all power-generating facilities.

Background checks: Some specific recommendations

On the subject of creating a situation which would make it possible for employers to perform background checks, Mr. Jan Larson, Security Director for the Pfizer Corp., said:

I feel that it is not a deterrent to crime if an employee is apprehended in a criminal act and he knows that his criminal history will not follow him. This knowledge should give

him a secure feeling and possibly an incentive to continue in his area of crime, to know that if and whenever he is apprehended his crime will remain a secret. I have my own thoughts on the cataloging and retention of criminal records.

Mr. Ross also called for access to criminal background information, but in doing so he made a concrete proposal for limiting the possibility of abuse. Mr. Ross testified:

We in the private sector must also have the tools to cut costs; and it is within the power of you gentlemen to give them to us. You have stated sanctions and penalties against public law enforcement professionals for abuse of the Privacy Act information. Could you not also specify sanctions and penalties against private sector professionals who abuse Privacy Act information, but make it legal for us to have access to it?

Mr. Baird recommended legislation which would compel corporations to report crimes. He testified:

In my judgment, the legislation before the Senate needs to be amended to apply the same criminal sanctions against the management of a corporation and/or its data processing manager for the failure to report to the proper authorities criminal activity of some magnitude.

If procedures which make meaningful background checks on employees possible are ever to be established, it will require in the first instance some amendments to the privacy legislation now on the books.

Beyond this, and perhaps much more difficult, it will require uniform State legislation.

It should be noted that the security experts who testified were not calling for access to confidential law enforcement information for backgrounding purposes. What they were talking about was access to public record data on arrests, indictments, and convictions. Such data is on file at county courthouses around the country—and if an employer could afford the expense of searching through the records in the many thousands of county courthouses and then pulling together the information, he would, theoretically, be able to do an effective job of backgrounding on any applicant for a position where a meaningful background check was indicated.

Clearly, this is impossible. Some employers will go to the trouble of checking the criminal records in a single jurisdiction—in most cases where the applicant resided for the longest period of time. This is the practice followed by Equifax and Fidelifax and other companies which conduct background checks for a fee. Such a limited check has its utility, particularly in dealing with applicants who have resided in one place and worked for a single employer for long periods of time. Certainly, it is better than nothing. On the other hand, it is clearly inadequate when one is dealing with sensitive positions and contending with criminal elements and more mobile backgrounds.

The National Crime Information Center of the Department of Justice in 1971 established the Computerized Criminal History (CCH) file as part of its criminal information system. The CCH operation brings together from all over the Nation offender criminal histories, including arrests, indictments and convictions. This information is

available on demand to law enforcement agencies at the Federal, State and local level through thousands of user terminals. Noting that such a centralization was essential in order to contend with increasing criminal mobility and the high rate of recidivism, an official paper put out by the NCIC Advisory Board spoke of "the need to develop an offender criminal history exchange with the States that will rapidly gain the confidence of all users in terms of system integrity, accuracy, and completeness of file content."

Private employers have not had access to the CCH file, even when they have been seeking to do background check on applicants for highly sensitive positions. The absolute prohibition which exists today on access to CCH information by private employers does not rest on the confidentiality of this information. It is, as has been pointed out above, a matter of public record—but scattered around the country through thousands of legal jurisdictions. It seems paradoxical that an access which is legal at the local or State level should be prohibited at the point where the information is nationally centralized. The question is whether legislation could be devised that would make such access possible, under very careful guidelines, limited to certain categories of employment where a careful check of criminal records is essential in the interest of protecting the public.

The alternative to such legislation is the perpetuation of the status quo, which makes meaningful background checks impossible—no matter what degree of risk this may pose to the public, the community, and the Nation.

XI. CONSEQUENCES OF THE EROSION (IV): THE DISMANTLING OF THE FEDERAL EMPLOYEE SECURITY PROGRAM

In the course of looking into the impact which the erosion of law enforcement intelligence has had on the Federal Loyalty-Security Program the Subcommittee discovered that, for all practical purposes, nothing remains of the program established by legislation or by Executive Order.

After taking the testimony of Mr. Alan K. Campbell, Chairman of the U.S. Civil Service Commission, Senators Eastland and Thurmond, in a joint letter, dated March 1, 1978, wrote to Mr. Campbell that they "were profoundly disturbed by some of the answers which you and Mr. Drummond gave in the course of your testimony." Summarizing the testimony presented by Mr. Campbell, Senators Eastland and Thurmond said:

In the light of this information, we find it difficult to avoid the conclusion that over the past 5 years or so, without the knowledge of Congress and contrary to statutory requirements and the Commission's own regulations, there has been a progressive dismantling of the Federal Loyalty-Security Program—until today, for all practical purposes, we do not have a Federal Employee Security Program worthy of the name.

In one form or another there has been a long-standing requirement that those employed by the Federal Government be reliable, trustworthy, and loyal to the United States of America. Paragraphs dealing with these requirements are to be found in the Civil Service Act of 1883. By the early 1950's, there were at least eight additional laws and a series of Executive orders dealing with different aspects of the problem.

In April of 1953, President Eisenhower sought to bring some order into the Government's Loyalty Security Program by promulgating Executive Order 10450. By way of explaining the motivation for the Executive order, President Eisenhower said in his 1953 State of the Union Message:

The safety of America and the trust of the people alike demand that the personnel of the Federal Government be loyal in their motives and reliable in discharge of their duties. Only a combination of both loyalty and reliability promises genuine security.

Since 1953, Executive Order 10450 has undergone a series of amendments, suggested both by practical experience and by several Supreme Court decisions. The criticism has been made that, even with these amendments, the Executive order is out-of-date and that it requires further amendment, or even rewriting, in order to make it a viable administrative and legal instrument. However, as amended, it still remains the law of the land and the presumed guiding authority

for the various executive agencies in the conduct of their own employee security programs.

The key paragraphs of Executive Order 10450, as currently amended, read as follows:

Whereas the interests of the national security require that all persons privileged to be employed in the departments and agencies of the Government, shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States; and

Whereas the American tradition that all persons should receive fair, impartial, and equitable treatment at the hands of the Government requires that all persons seeking the privilege of employment or privileged to be employed in the departments and agencies of the Government be adjudged by mutually consistent and no less than minimum standards and procedures among the departments and agencies governing the employment and retention in employment of persons in the Federal service:

* * * * *

Section 2.—The head of each department and agency of the Government shall be responsible for establishing and maintaining within his department or agency an effective program to insure that the employment and retention in employment of any civilian officer or employee within the department or agency is clearly consistent with the interests of the national security.

* * * * *

(b) The head of any department or agency shall designate, or cause to be designated, any position within his department or agency the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security, as a sensitive position. Any position so designated shall be filled or occupied only by a person with respect to whom a full investigation has been conducted.

* * * * *

Section 5.—Whenever there is developed or received by any department or agency information indicating that the retention in employment of any officer or employee of the Government may not be clearly consistent with the interests of the national security, such information shall be forwarded to the head of the employing department or agency or his representative who, after such investigation as may be appropriate, shall review, or cause to be reviewed, and, where necessary, readjudicate, or cause to be readjudicated, in accordance with the said act of August 26, 1950, the case of such officer or employee.

The language of Executive Order 10450, it is to be noted, did not automatically bar applicants from Federal employment if they had at some time in the past been members of subversive organizations. It made allowance for the fact that many people join such organizations

in innocence, attend perhaps a few meetings, and then drop out. The Order spelled out a number of factors that were to be taken into consideration by agency heads and it made it clear that each case had to be considered on its own merits, taking into consideration the separate facts and circumstances.

Over the past decade or more there has been a progressive retreat from the intent and provisions of Executive Order 10450 and from the entire concept of personnel security in government. This retreat has paralleled the general erosion of law enforcement intelligence and to a large degree must be considered a consequence of this erosion.

In its own right, Executive Order 10450 must also be regarded as a law whose effective implementation is impossible without an orderly gathering and dissemination of intelligence. To help meet this requirement, the Civil Service Commission maintained a number of file systems. One of these systems, according to the testimony of Mr. Campbell, contained "the name of the individual and a brief description of his or her activities . . . which provided a lead to a file containing detailed information about the organization, event, or publication." Mr. Campbell said that a subject's name would be checked against the index routinely during the course of an investigation.

The second set of files maintained by the Civil Service Commission brought together information on numerous extremist organizations of the far left and the far right.

Mr. Campbell told the subcommittee that use of the personal index system was terminated by the Commission "pursuant to section (e)(7) of the Privacy Act." He also stated that although the Civil Service Commission still retained its organizational files, "the Commission has notified GAO that it will adopt the GAO recommendation to dispose of these files also." (Actually GAO did not recommend that the files be destroyed; it recommended that the Civil Service Commission "obtain authorization from Congress for the files on alleged subversive and radical organizations, or delete them.")

Commenting on the reported or threatened destruction of the files, Senators Eastland and Thurmond said in their letter of March 1, 1978:

. . . It was unclear whether they have been physically eliminated or simply locked up or whether you contemplate their physical elimination.

We ask that you postpone taking any irrevocable action with regard to the files currently in your possession until Congress has had an opportunity to consider the matter and make a finding.

In his oral testimony and in his responses to a long series of written questions, Mr. Campbell detailed the erosion that had taken place in the Commission's ability to conduct background checks on applicants for Federal employment.

He said, as noted above, that the Commission no longer checks its Security Research Files because the index to these files was eliminated pursuant to section (e)(7) of the Privacy Act. He also said the House Internal Security Committee files, which the Commission previously used to check, are no longer available.

Mr. Campbell noted, too, that the Civil Service Commission runs into many obstacles when it seeks to obtain information from law enforcement agencies, schools, and other sources. Speaking about the falloff in cooperation which the Civil Service Commission had experienced, Mr. Campbell said:

. . . An ever growing number of employers refuse to respond because of the disclosure provisions of the Privacy Act. A large and growing number of colleges and universities refuse to respond citing either the Privacy Act or the Education Act as the reason. Most individuals still respond . . .

Mr. Campbell was asked whether a GAO report of December 16, 1977 was accurate when it described the restriction of access to local law enforcement records in these terms:

Due to legal constraints and nonresponses to inquiries, CSC cannot check some local enforcement records, even though the check is required by Executive Order 10450. By September 1976, the Chicago area [of CSC] had stopped sending [requests for information] to law enforcement agencies in New York, California, Minnesota, New Mexico, Massachusetts, and Illinois, and 86 cities in other States, because the agencies refused to release criminal information to CSC. Some of the larger cities are Detroit, Indianapolis, and Washington, D.C. Thus, an investigation cannot surface criminal information on individuals who reside in these areas, unless the information is also on file with the FBI.

Mr. Campbell responded that this is an accurate description of the situation which existed in September 1976 and that things had not improved since that time.

Another difficulty referred to by Mr. Campbell had to do with obtaining information from State sources governed by highly restrictive state statutes on the dissemination of information. "For example," he said—

the State of Massachusetts has a law which provides that only recognized criminal justice agencies may get police information. At one time we were recognized by the board up there, but they withdrew this recognition, and we can no longer get criminal justice information from the State of Massachusetts, except by going to the courts.

According to Mr. Campbell, the reason cited most frequently by State and local authorities for withholding criminal justice information from the Civil Service Commission was the Law Enforcement Assistance Administration regulations, rather than the Privacy Act.

Even in those cases where the Civil Service Commission is able to obtain the cooperation of local law enforcement authorities, it is highly questionable whether the available information would satisfy the requirements of sound security practices. On this point, the following exchange took place:

Senator THURMOND. The subcommittee has heard from the intelligence units of many police departments that intelligence-gathering guidelines at State and local levels—in those cities and States that still do maintain domestic intel-

ligence files—have been watered down to the point where they cannot include information dealing with mere membership in organizations like the Communist Party, the Trotskyite Party, the Maoists, the Puerto Rican Socialist Party, the KKK, the American Nazi Party, the Jewish Defense League, and the Palestine Liberation Organization. They cannot make an intelligence entry about membership in such organizations, unless there has been an indictment or conviction.

If local and State organizations, because of the guideline restrictions that have been posted in recent years, cannot maintain such intelligence, obviously there is no way they can pass intelligence on to you, is there?

Mr. CAMPBELL. That is correct.

The Civil Service Commission is further hampered in its investigations under current procedures governing the implementation of the Privacy Act. Mr. Campbell testified that whenever a Civil Service Commission investigator goes to a source or witness, "he must first advise them of the Privacy Act and of the fact that the information that they give, as well as their identity, would appear in a report of investigation and be furnished to the subject if he or she so requests." A pledge of confidentiality, said Mr. Campbell, could be given to a witness if he asks for it, but investigators are instructed not to raise the matter of confidentiality.

The questioning revealed that, over and above all of the restrictions that today govern the backgrounding of applicants for Federal employment, the Civil Service Commission's own criteria have been watered down to the point where they have become meaningless. Summarizing the testimony on this point, Senators Eastland and Thurmond said in their letter of March 1, 1978:

You were asked whether loyalty to the U.S. Government was still a condition of Federal employment—and you replied that it was. You next agreed that "the starting point of any intelligence operation relating to personnel security in Federal employment would be the establishment of certain criteria or guidelines." But then you testified that you did not have any such criteria.

Then it emerged that as matters now stand you do not even ask questions of applicants for sensitive positions whether they are or have been members of Communist or Nazi or other totalitarian or violence-prone organizations—that, in the absence of an overt act, mere membership in such organizations would not disqualify a person for Federal employment. In the course of the questioning, we mentioned quite a number of organizations—the American Communist Party; the KKK; the American Nazi Party; the Maoists; the Trotskyists; the Prairie Fire Organizing Committee—which publicly supports the terrorist activities of the Weather Underground; the Puerto Rican Socialist Party—which similarly supports and defends the violence perpetrated by the Puerto Rican terrorists; the Jewish Defense League—which engages, in its own name, in acts of violence; and the Palestine Liberation Organization—whose American affiliates

support the terrorist acts perpetrated by its parent organization in other countries. The same answer, apparently, applied to all organizations: In the absence of an overt act, mere membership is not a bar to Federal employment.

On the question of mere membership, Mr. Drummond at one point stated that, if it were discovered that an applicant was a member of the KKK, he probably would not be considered suitable for a job with the Equal Employment Opportunities Commission—although his membership would apparently be no bar to employment in other Government positions, even sensitive positions. What Mr. Drummond did not explain was how you could possibly find out that an applicant was a member of the KKK if you cannot ask the applicant or those who know him any questions about mere membership in any organization. Nor did Mr. Drummond offer any example of the kind of employment for which “mere members” of the many other organizations of the far left and the far right might be found unsuitable.

At points in their testimony, Mr. Campbell and Robert J. Drummond, Jr., Director of the Bureau of Personnel Investigations, who accompanied him, appeared to be telling the subcommittee that they had some flexibility in making notations about membership in extremist organizations, even in the absence of overt violations of the law. At other points, they stated quite explicitly that “mere membership” in an extremist organization was not enough to warrant a notation in the subject’s file. The following question and answer is an example of such an explicit statement:

Senator THURMOND. And you would not maintain in your files the information that a man is a member of the Communist Party or any organization that stands for the violent overthrow of our Government. Mere membership would not be enough to allow you to put that in your files—you would have to have some overt act?

Mr. DRUMMOND, Yes. We would have to have something more than the mere membership.

The subcommittee has no question but that there does, in fact, exist an absolute “taboo” in the Civil Service Commission on all investigative information dealing with what is euphemistically called “mere membership” in extremist organizations. Civil Service Commission investigators who were interviewed by the subcommittee staff said that, under today’s rules, if an applicant’s neighbor told them that he had known the applicant as an active member of the Ku Klux Klan or the Communist Party for 20 years, no notation to this effect could be made in the absence of an overt violation of law resulting in an indictment or conviction. A Civil Service Commission Investigator’s Manual of June 10, 1977, which was provided to the subcommittee, contains these instructions for investigators:

(a) Members of the local chapter of an organization are reported to have visited the house of a witness who is expected to testify at an upcoming trial and threaten bodily harm if the witness testifies. If the subject of an investigation is reported to be a member of the chapter, our inquiry must be

limited to subject's activities, if any, in connection with the visit to the home of the witness.

(b) Members of an organization are reported to have set fire to the campus ROTC building. If the subject of investigation is reported to be a member of this group, our inquiry would be limited to his/her activities, if any, in connection with the act of arson.

* * * * *

In summary, the basic report of investigation should never contain information which reports that the subject is or is not a member of any organization merely for the purpose of covering outside activities or for the purpose of reporting the subject's political, religious, fraternal, civic, sociological, or racial views or connections, regardless of the fact that the investigator or the witness may personally believe that such views or activities, even though legal, reflect unfavorably on the subject's loyalty.

Mr. Drummond told the subcommittee that one of the reasons for disqualifying an applicant is "reasonable doubt as to loyalty of the individual to the Government."

But then he went on to say:

As pointed out in the answers to the questions, there has not been an individual removed from Federal service or denied appointment to the Federal service on the basis of reasonable doubt as to loyalty, during the past 10 years.

As a matter of fact, from 1956 to 1968 there were only 12 applicants denied employment and 4 appointees removed from employment on the basis of reasonable doubt as to loyalty.

There were 510 applicants whose loyalty may have been questioned in addition to those 12, but they were removed on other suitability grounds. This could have been for criminal conduct. It could have been because of delinquency or misconduct in prior employment.

Nevertheless, there was a loyalty question, but CSC chose to use other suitability grounds for their removal, resulting in only 12 being removed because of reasonable doubt as to loyalty.

I think the reason for this is that there has been a reluctance over the whole history of the security program to stigmatize some individual with the disloyalty label when there is some other way in which he can be removed or denied employment. I think this is general knowledge.

Applicants for nonsensitive positions are subject to what is called a National Agency Check and Information (NACI) investigation, while applicants for sensitive positions are subject to full field investigations. The GAO reported that during the fiscal year 1976 the Civil Service Commission conducted 336,321 NACI investigations and 26,903 full field investigations, at a total cost of \$23.5 million. The question that must be raised is whether these checks have any substantive value at all in terms of protecting the Government against infiltration by hostile agents and ideological extremists of the far left and the far right.

The series of circumstances and decisions that brought the Federal Employee Security Program to this lamentable state cannot be attributed to any single agency or any single administration. It is the product of a complex of developments, involving both Democratic and Republican Administrations, decisions of the Supreme Court, the Privacy Act and the Freedom of Information Act, and arbitrary rulings by the Counsel for the Civil Service Commission, putting the most restrictive interpretations on Supreme Court decisions and the requirements of the privacy legislation.

The Commission, acting on advice of its Counsel and officers, has, in fact, directly contributed to this dismantlement in three different ways: (1) it has placed an excessive interpretation on the requirements of the Privacy Act and on several of the more restrictive Supreme Court decisions; (2) it has ignored other Supreme Court decisions belonging to roughly the same time frame that had to do with the nature of the Communist movement, the responsibility of Government to protect itself against infiltration by hostile elements, and the basic legal purposes of the Subversive Activities Control Act; and (3) it has in a series of situations surrendered important components of the loyalty security program on the ostensible excuse that the Civil Service Commission would not be sustained if a challenge were brought in the courts.

A November 12, 1973 memorandum entitled "Revisions of Loyalty Questions on SF-171" signed by Bernard Rosen, Executive Director of the Civil Service Commission, said:

Recent decisions of the Supreme Court make it clear that mere membership in an organization that espouses the unlawful overthrow of the Government may not be inquired into, and that the only fact of relevance is membership with knowledge of the unlawful purpose of the organization, and with specific intent to carry out that purpose. To effect changes in the loyalty questions (27 and 28) on Standard Form 171 (September 1971) reflecting the court decisions, the Civil Service Commission, with approval of the Justice Department as to their format, has revised questions 27 and 28.

The revision of questions 27 and 28 on Standard Form 171 will also apply to similar loyalty questions on other application or appointment forms under the Civil Service Commission's jurisdiction, such as Standard Forms 173 and 50A and any exceptions to those forms granted to agencies.

Questions 27 and 28 dealt with membership in the Communist Party, U.S.A., or other organizations advocating the use of force for political change. In an effort to rewrite these questions in a manner conforming with the Supreme Court ruling, question 28 was broken down into three parts, in a manner which placed emphasis on knowledge of the unlawful purpose of the organization in question and on the applicant's intent to carry out that purpose. The revised question 28 read:

28. (a) Are you now, or within the last 10 years have you been, a member of any organization, or group of persons, including but not limited to the Communist Party, U.S.A.,

or any subdivision of the Communist Party, U.S.A., which during the period of your membership you knew was advocating or teaching that the Government of the United States or any political subdivision thereof should be overthrown or overturned by force, violence, or any unlawful means?

28. (b) If your answer to (a) is in the affirmative, did you, during the period of such membership, have the specific intent to further the aims of such organization or group of persons to overthrow or overturn the Government of the United States or any State or any political subdivision thereof by force, violence, or any unlawful means?

28. (c) If your answer to 27 or 28(a) above is in the affirmative, state the names of such organizations and the date of your membership in each in item 37 or other space provided for detailed answers.

This attempt to retain something of the question having to do with loyalty to the U.S. Government was dealt another blow by the Privacy Act of 1974, or, to be more precise, by the Commission's interpretation of its requirements. Section 552a(e)(7) of the Privacy Act requires Government agencies to—

Maintain no record describing how any individual exercises rights guaranteed by the first amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of authorized law enforcement activity.

In a memorandum, dated February 18, 1975, dealing with the implications of the Privacy Act for the Civil Service Commission, Robert J. Drummond, Jr., Director of the Bureau of Personnel Investigations, noted that the legislation "impacts on just about everything the Commission does with respect to the collection, maintenance, use and dissemination of personal information". He went on to say that the act "raises serious questions as to the legality" of continuing to maintain the Security Research and Analysis Index. [This Index, which was maintained by the Security Research and Analysis Section, was an investigative leads file containing information relating to Communist and other subversive activities].

Under the Privacy Act of 1974, said Mr. Drummond, the Commission would be required to publish annually in the Federal Register a notification that included (1) the categories of individuals on whom records were maintained, (2) a description of the routine usage of these records, (3) the procedures to be employed by an individual wishing to be notified if there was any record on him in the file and (4) the manner in which an individual may gain access to any record pertaining to him and contest its contents. Mr. Drummond expressed the fear that to keep the file would expose the CCS to innumerable court challenges.

In the closing paragraph of the memorandum, Mr. Drummond remarked:

Over the years, the Bureau of Personnel Investigations has taken great pride in the Security Research and Analysis Section. We have had the good fortune to have it staffed by dedicated people. . . . Nevertheless, I feel that in spite of

any benefit we may derive from the file and no matter what safeguards we apply to collecting, maintaining, using and disseminating such information, the time has come to discontinue its maintenance and use.

After a period of consideration, a decision was finally made. Bulletin No. 736 of September 9, 1975, signed by Raymond Jacobson, executive director, instructed:

Effective September 9, 1975 the Index will no longer be searched as part of any Commission investigative effort (National Agency Checks, full field background investigations, suitability investigations) nor will the Commission search the Index as part of an agency's investigative effort. *The Security Research staff will continue to maintain files on organizations and this information will be given to agencies upon request. However, these organizational files will not be cross-indexed in any manner to individuals.* (Emphasis from original).

In 1976 and 1977, the retreat from sound personnel security practices was converted into a rout. CSC Bulletin No. 295-33, dated October 21, 1976, instructed the heads of all departments and independent establishments that loyalty questions were to be completely eliminated from application forms for employment in the Federal Civil Service. The key paragraphs read:

The Civil Service Commission is eliminating loyalty questions 27, 28a, 28b, and 29 on Standard Form 171, Personal qualifications Statement (May 1975 edition) and similar questions on all other Federal application forms used in the competitive service. The conviction question is also modified to conform with revised suitability guidelines issued in FPM letter 731-3, dated July 3, 1975.

. . . Civil Service Commission examining offices will no longer gather information nor initiate actions regarding loyalty determinations. Such determinations will now be made at the time of suitability investigations or during the agency selection process. The Bureau of Personnel Investigations will continue to be responsible for adjudicating all loyalty cases.

In implementation of this directive, the following item was included in a supplemental page appended to the Federal employment application statement:

Loyalty—(Items 27, 28, and 29 on SF-171, May 1975 edition, and Item 15 on SF-173, July 1968 edition.) Recent court decisions have prohibited routine inquiry into an individual's membership in certain organizations. As a result, questions on the Federal application form concerning membership in (a) the Communist Party, U.S.A., or (b) organizations advocating the overthrow of the Government of United States or any of its subdivisions, should not be answered. However, if you are under consideration for appointment to sensitive positions for which such associations would be of relevant concern, you may be asked to provide

such information. Do not answer the questions—cross them out on the qualifications statement.

On October 31, 1977, the caveat that had previously permitted the asking of questions regarding organizational affiliation where sensitive positions were involved, was eliminated in a directive from Raymond Jacobson, Executive Director of the Commission, to heads of departments and independent establishments. Bulletin No. 736-8 conveyed this instruction:

The Civil Service Commission is eliminating the requirement to answer questions 21, 22, 23 and 24 on Standard Form 86, Security Investigation Data for Sensitive Positions (August 1964 edition).

In making their decision, the Commissioners accepted the legal opinion of the Commission's General Counsel that question 21 has a chilling effect on First Amendment Rights and question 22 is unconstitutionally vague. . . .

This is where our Federal Employee Security Program stands today.

The question must be raised whether all of the retreats ordered by the Civil Service Commission were really made mandatory by Supreme Court decisions and by the Privacy Act. The Civil Service Commission is responsible to Congress and to the Nation for administering the various statutes dealing with the requirement of loyalty on the part of Government employees and the establishment of sound personnel security practices. It should have been the function of the Commission to defend the Government's Personnel Security Program by resisting the abandonment of essential components unless this abandonment was ordered by the courts. Instead, it is difficult to escape the impression that, through the series of incremental orders and directives quoted above, the Commission has effectively abandoned its entire Personnel Security Program without putting up a fight and without calling the dismantling of the program to the attention of Congress..

Hopefully, sound personnel screening procedures still exist in the CIA, the National Security Agency, the FBI, and DOD, and several other Government agencies which conduct their own clearances and which are not governed by civil service interpretations. Civil Service Commission procedures do apply, however, for the majority of Government agencies, including highly sensitive agencies like the State Department and the Energy Administration. Even in the case of the Department of Defense, the subcommittee was informed, Civil Service Commission personnel security criteria govern the hiring of all civilian personnel. This holds true, apparently, for highly sensitive positions as well as nonsensitive positions. One such situation was called to the attention of the subcommittee by two former computer security evaluators for the United States Army, Mr. James R. Wade, and Mr. Frederick G. Tompkins.

In a signed statement on October 20, 1978, Mr. Wade, and Mr. Tompkins informed the subcommittee that recently there was an opening in a critical intelligence operation for three computer security specialists. Army security officers were told by the local Civilian Personnel Office that, based on Civil Service Commission policy, clear-ability for defense information security clearances "could not be used as a criterion for employment". The function of a computer security specialist is to protect computer systems against hostile

penetration. It would be difficult to conceive of a function more critical or more sensitive. But in this instance the Army was being told that, even if an applicant was found ineligible for clearance by Army standards, this fact could not be used to bar his employment.

In the low security, and even nonsecurity, climate in which Government personnel operate today, all kinds of other departures from sound security practices inevitable occur. Mr. Wade and Mr. Tompkins also expressed their concern about uncleared civilian maintenance personnel gaining access to extremely sensitive computer systems. Their statement said:

. . . Most computer hardware vendors clear a minimum number of computer maintenance personnel in any one geographic location; therefore, when one or more of these cleared individuals are unavailable due to sickness, vacation, et cetera, the vendor will provide a qualified but not necessarily cleared substitute. DOD instructions permit such practices; however, they do require a cleared escort to accompany the uncleared person. In practice it is lower graded personnel who can be spared most readily that are usually assigned such escort duties. Additionally, escorts do not normally possess sufficient technical knowledge to properly or adequately determine that the uncleared maintenance personnel are not making unauthorized modifications to equipment. In some cases, processing of classified material has continued during the presence of uncleared vendor maintenance personnel. Such practices raise the risk of unauthorized disclosure of classified/sensitive data to a questionable level. Permitting uncleared personnel of any category to gain access to ADP systems that are processing sensitive information diminishes the Federal personnel clearance program effectiveness and seems to violate the intent of the Office of Management and Budget (OMB) Circular A-71, subject: Security of Automated Information Systems, dated: July 27, 1978.

Summarizing the contradictory position in which the various computer security programs operated by the executive branch and its departments now find themselves, Mr. Wade and Mr. Tompkins noted that OMB Circular A-71, which is supposed to establish policy and responsibility for the development and implementation of Government security computer programs, has one section which requires each agency "to establish personnel security policies for screening all individuals participating in the design, operation, or maintenance of Federal computer systems, or having access to data in Federal computer systems"; and it has another clause which has the effect of restricting access to personal data about such people even where personnel security investigations are involved. The paradox created by these two conflicting requirements is apparently being resolved in favor of the right of personal privacy as opposed to the requirement of national security.

RECOMMENDATIONS

In reconstructing the Federal Employee Security Program, we must start today from ground zero. The General Accounting Office (GAO) in a report, dated December 16, 1977, recommended that "the Congress should consolidate into one law the authority to investigate and

judge the suitability of Federal employees, including the potential of employees in sensitive positions to impair national security." It further recommended that Congress consider the impact of the restrictions imposed on personnel investigations by the Privacy Act of 1974 and other laws, and of court decisions protecting the constitutional rights of the individual. It also suggested that Congress consider the "need to define, in a manner acceptable to the courts, disloyal acts which should bar Federal employment"; and that it might wish to establish several different levels of investigation for Federal employees depending on the sensitivity of their positions.

Even these recommendations, however, do not provide a total answer to the problem of reconstructing the Federal Employee Security Program in a manner which: (1) Acknowledges the privilege of Federal employment; (2) protects the rights of applicants seeking Federal employment, and (3) at the same time protects the public's right to national security.

It will also be necessary for the Congress to mandate in clear and concise language who has the authority to establish guidelines and to gather, receive, maintain, analyze, use, and disseminate to Government agencies intelligence information related to the operation of a Federal Employee Security Program. In addition, the problem of insuring the anonymity of those who provide information must be confronted in a positive and forthright manner.

APPENDIX

[Report by the Comptroller General of the United States]

DATA ON PRIVACY ACT AND FREEDOM OF INFORMATION ACT PROVIDED BY FEDERAL LAW ENFORCEMENT AGENCIES

The Chairman, Senate Committee on the Judiciary, asked GAO to obtain data showing the fiscal impact on some law enforcement agencies resulting from the response to individuals requesting information or access to agency records and files.

Thirteen agencies contacted by GAO either estimated or identified operating and start-up costs associated with the two acts to be \$35.9 million during a 3-year period beginning in 1975 and ending in 1977. Agency operating costs ranged from about \$159,000 to \$13.8 million. About 80 percent of the operating costs of the agencies reporting cost breakdowns went for salaries.

During the period 1975-77, the 13 agencies reported receiving about 147,000 requests. The most dominant category of requesters identified by many of the agencies was individuals who have been or are subjects of Federal investigations by the agencies. Some of these requesters were also identified by agencies as being criminals.

SCHEDULE A.—SUMMARY OF FOIA AND PA REQUESTS AND COST DATA

Agency	Period ¹	Operating costs			Startup costs ²	Period ¹	Number of requests		
		PA	FOIA	Total			PA	FOIA	Total
Department of Justice: Federal Bureau of Investigation ³	Fiscal year 1975			\$455,353		October 1974 to September 1975			10,522
	Fiscal year 1976			3,269,000		October 1975 to September 1976			15,304
	Transition quarter			906,081		Fiscal year 1977			17,540
	Fiscal year 1977			9,119,983					
				13,750,417					43,366
Drug Enforcement Administration	September 1975 to September 1976			508,452	\$148,015	Calendar year 1975	146	529	675
	Fiscal year 1977			832,000		Calendar year 1976	619	144	763
						January to September 1977	503	124	672
				1,340,452	148,015		1,268	797	2,065
Immigration and Naturalization Service	Fiscal year 1976	\$101,517	\$113,999	215,516	141,074	Fiscal year 1976	6,898	11,634	18,532
	Transition quarter	102,512	42,000	144,512		Transition quarter	3,427	2,754	6,181
	Fiscal year 1977	300,000	150,000	450,000		Fiscal year 1977	15,986	10,500	26,486
		504,029	305,999	810,028	141,074		26,311	24,888	51,199
Department of the Treasury: Secret Service	Fiscal year 1975		29,142	29,142	3,321	May to September 1975		375	375
	July 1975 to September 1976	165,838	183,863	349,701	24,850	October 1975 to September 1976	222	837	1,059
	Fiscal year 1977	154,714	164,368	319,082		Fiscal year 1977	301	946	1,247
	320,552	377,373	697,925	28,171		523	2,158	2,681	
Bureau of Alcohol, Tobacco and Firearms	Fiscal year 1975		24,000	24,000		Fiscal year 1975		76	76
	July 1975 to September 1976	228,400	106,850	335,250	138,039	July 1975 to September 1976	367	384	751
	Fiscal year 1977	195,450	97,550	293,000		Fiscal year 1977	409	465	874
	423,850	228,400	652,250	138,039		776	925	1,701	
U.S. Customs Service	Fiscal year 1975					Fiscal year 1975			645
	October 1975 to September 1976	500,000	1,300,000	1,800,000		July 1975 to June 1976			1,253
	October 1976 to September 1977	533,000	1,546,000	2,079,000		July 1976 to July 1977			2,205
		1,033,000	2,846,000	3,879,000					4,103
Internal Revenue Service	Calendar year 1975	(?)	2,700,000	2,700,000		Calendar year 1975		15,540	15,540
	Calendar year 1976	500,000	2,700,000	3,200,000		Calendar year 1976	925	9,687	10,612
	Calendar year 1977	900,000	2,900,000	3,800,000		Calendar year 1977			
		1,400,000	8,300,000	9,700,000			925	25,227	26,152
U.S. Postal Service: Inspection Service	October 1975 to September 1976	18,150	60,322	78,472	17,444	October 1975 to September 1976	45	437	482
	October 1976 to September 1977	1,432	78,925	80,357		October 1976 to September 1977	27	478	505
		19,582	139,247	158,829	17,444		72	915	987
Department of Defense: Defense Investigative Service	Fiscal year 1975		14,196	14,196		Fiscal year 1975		143	143
	Fiscal year 1976	869,913	15,844	885,757	79,342	Fiscal year 1976	954	200	1,164
	Transition quarter	190,866	577	191,443		Transition quarter	302	16	318
	Fiscal year 1977	778,186	1,552	779,738		Fiscal year 1977	1,332	55	1,387
		1,838,965	32,169	1,871,134	79,342		2,598	414	3,012
Naval Investigative Service	Calendar year 1975	38,232	69,627	107,859	42,633	Calendar year 1975	156	191	347
	Calendar year 1976	145,000	23,757	168,757		Calendar year 1976	656	116	772
	Calendar year 1977	180,514	58,912	239,426		Calendar year 1977	798	230	1,028
	363,746	152,296	516,042	42,633		1,610	537	2,147	
Air Force Office of Special Investigations ³	Fiscal year 1975			39,775		Fiscal year 1975			622
	Fiscal year 1976			120,767		Fiscal year 1976	649	273	922
	Transition quarter			30,312		Transition quarter	34	201	235
	Fiscal year 1977			121,531		Fiscal year 1977	149	896	1,045
			312,385			832	1,370	2,202	
Army Criminal Investigations Command	Calendar year 1975	33,700	180,000	213,700		Calendar year 1975	94	374	468
	Calendar year 1976	66,600	159,300	225,900		Calendar year 1976	578	242	820
	Calendar year 1977	89,000	149,400	238,400		Calendar year 1977	545	255	800
	189,300	488,700	678,000			1,217	871	2,088	
Army Intelligence Security Command	Fiscal year 1975		116,793	116,793		Calendar year 1975	383	814	1,197
	Fiscal year 1976	193,253	106,722	299,975		Calendar year 1976	1,687	435	2,122
	Fiscal year 1977	369,525	157,181	526,716		January to October 1977	1,413	604	2,017
	562,788	380,696	943,484			3,483	1,853	5,336	
Grand total			35,300,946	594,718					147,039

¹ Agencies did not always maintain or estimate cost and request data on a fiscal year basis; some used a calendar year or a 12-mo period following the September 1975 effective date of the Privacy Act; and some reported data for the fiscal transitional quarter July to September 1976.

² Startup costs for the 2 acts were not separately identified by most agencies.

³ The Air Force, Office of Special Investigations and Department of Justice agencies, the FBI, and

DEA, generally did not report cost data separately for administering requests under the 2 acts. Also, the FBI did not segregate requests under the 2 acts.

⁴ Includes cost of \$2,000,000 to \$8,000,000 in fiscal year 1977 for a 1-time special effort (task force) to reduce the FBI's backlog of requests.

~~RESTRICTED~~
 This is a report on the results of work performed pursuant to a request of the committee on law enforcement
 which is printed here for the reasons of this report.

REPORT BY THE

Comptroller General

OF THE UNITED STATES

Impact Of The Freedom Of Information And Privacy Acts On Law Enforcement Agencies

Law enforcement officials almost universally agree that the Freedom of Information and Privacy Acts have eroded their ability to collect and disseminate information. However, the extent and significance of the information not being gathered because of these acts cannot be measured.



GGD-78-108
 NOVEMBER 15, 1978



COMPTROLLER GENERAL OF THE UNITED STATES
WASHINGTON, D.C. 20548

B-179296

The Honorable James O. Eastland
Chairman, Committee on the Judiciary
United States Senate

Dear Mr. Chairman:

In response to your April 1978 request, we are reporting on the impact the Freedom of Information and Privacy Acts are having on Federal law enforcement agencies' ability to obtain and exchange information.

Law enforcement officials almost universally believe that the ability of law enforcement agencies to gather and exchange information is being eroded. The extent and significance of the information not being obtained, however, cannot be measured. Some confusion also exists about the requirements and provisions of these acts that affect the ability of law enforcement agencies to collect and disseminate information.

Appendix I shows information obtained from law enforcement agencies, including typical examples of the effect that the Freedom of Information and Privacy Acts are having on their ability to (1) obtain information from the general public, informants, and businesses and institutions and (2) exchange information with Federal, State, and local agencies, and foreign governments. Additional examples are included in appendix II. As agreed with your office, we did not verify or draw conclusions from the examples provided. Further, we did not attempt to evaluate the benefits to be derived from these acts.

Our work was performed at the headquarters and selected field offices in California and the Washington, D.C., area of the Federal Bureau of Investigation; Drug Enforcement Administration; Bureau of Alcohol, Tobacco and Firearms; United States Secret Service; and Civil Service Commission. We interviewed agency officials and obtained examples of investigative cases affected by these acts. We also contacted State and local law enforcement agencies in California, Maryland, and Virginia to determine how the Freedom of Information and Privacy Acts were affecting their relationships with the Federal law enforcement agencies.

B-179296

As arranged with your office, unless you publicly release its contents, we plan no further distribution of this report until 30 days after its issue date. At that time, we will send copies to interested parties and make copies available to others upon request.

Sincerely yours,
Thomas A. Blais

Comptroller General
of the United States

C o n t e n t s

	<u>Page</u>
APPENDIX	
I	IMPACT OF THE FREEDOM OF INFORMATION AND PRIVACY ACTS ON LAW ENFORCEMENT AGENCIES
	1
	Background
	1
	Nature of investigative operations
	2
	Officials assert erosion of law enforcement capabilities
	2
	Financial and administrative burden
	3
	Reduced ability to obtain information
	4
	Exchange of information affected
	10
	Agency comments and our evaluation
	14
II	SELECTED CASE STUDIES PROVIDED BY FEDERAL AGENCIES
	15
III	SUMMARIES OF THE FREEDOM OF INFORMATION ACT AND PRIVACY ACT
	25
IV	September 13, 1978, letter from the Civil Service Commission
	27
V	October 5, 1978, letter from the Department of the Treasury
	30
VI	October 26, 1978, letter from the Department of Justice
	33

ABBREVIATIONS

ATF	Bureau of Alcohol, Tobacco and Firearms
CSC	Civil Service Commission
DEA	Drug Enforcement Administration
FBI	Federal Bureau of Investigation
FOIA	Freedom of Information Act
GAO	General Accounting Office
IRS	Internal Revenue Service
PA	Privacy Act
USSS	United States Secret Service

IMPACT OF THE FREEDOM OF INFORMATION AND
PRIVACY ACTS ON LAW ENFORCEMENT AGENCIES

BACKGROUND

In the last 5 years the Congress has enacted legislation to control and provide public access to the vast amount of information collected, maintained, and disseminated by the Federal Government. The Congress intended this legislation to provide openness in Government activities and protect individual privacy.

These laws include the Freedom of Information Act (FOIA), enacted in 1966 and amended in 1974, which allows public access to information maintained by Federal executive agencies (see app. III); the Privacy Act (PA) of 1974, which emphasizes the protection of an individual's personal privacy by controlling the collection, maintenance, retention, and dissemination of personal information (see app. III); and the Tax Reform Act of 1976, which limits dissemination of tax returns and taxpayer information for non-tax-related matters. Many States have enacted their own openness laws to provide public access to State government records and activities and privacy laws to regulate the collection and dissemination of information by State agencies and by private organizations.

Law enforcement agencies depend on recorded information about the activities of individuals and desire full and complete access to such information while performing their legitimate law enforcement activities. Additionally, these agencies have traditionally been very protective of the information they collect and use and have worked under systems that promise total confidentiality. Therefore, such legislation as the FOIA and the PA, which opens records to public inspection and restricts the collection and flow of information, has a definite impact on how law enforcement agencies operate and fulfill their responsibilities.

Law enforcement officials at all levels of government have stated in congressional testimony that the proliferation of access and privacy laws has been instrumental in creating a restrictive climate which affects their ability to obtain information from the public and institutions, to recruit and maintain informants, and to exchange information with other law enforcement agencies.

NATURE OF INVESTIGATIVE OPERATIONS

Law enforcement agencies conduct criminal, as well as national security investigations. These investigations vary from relatively short-term efforts following a crime to long-term efforts sustained over a period of years. Efforts generally involve identifying perpetrators of violent and nonviolent crimes, developing evidence for prosecution, and gathering intelligence about individuals or organizations involved in, or contemplating involvement in, criminal activities. Investigations range from general criminal matters to organized crime, terrorism, political corruption, and foreign counterintelligence operations.

During investigations agencies must develop the pertinent facts in a given case. The development of these facts requires various investigative techniques, such as obtaining information from informants and other individuals who do not want their identities revealed, reviewing institutional records, and gathering information from the general public. Information developed through these efforts normally is systematically recorded and evaluated for use in current and future investigations. Additionally, law enforcement agencies disseminate information to other agencies with similar investigative interests to avoid duplication of investigative efforts.

OFFICIALS ASSERT EROSION OF LAW ENFORCEMENT CAPABILITIES

Federal and local law enforcement officials say the FOI/PA and similar laws are eroding their investigative capabilities, especially in the area of intelligence gathering. They believe the acts (1) are a financial and administrative burden, (2) inhibit their ability to collect information from the general public, informants, and institutions, and (3) diminish the quality and quantity of information exchanged with other law enforcement agencies.

Federal Bureau of Investigation (FBI) and U.S. Secret Service (USSS) officials indicate that the legislation is forcing them into a reactive rather than a preventive role and that the total effect of these laws has not and will not be realized until sometime in the future. The FBI, USSS, Drug Enforcement Administration (DEA), and Bureau of Alcohol, Tobacco and Firearms (ATF) officials have stated that they cannot measure the extent of the erosion or provide concrete evidence of its effects because they lack ways of determining the value or impact of the information not being received.

APPENDIX I

APPENDIX I

We asked the agencies for examples of how the acts have affected their investigative operations. Although several agencies provided examples showing the legislation's impact in specific cases, no agency could document the total impact the laws have had on overall investigative operations. Furthermore, it was difficult for them to distinguish between the impact resulting specifically from the FOI/PA provisions and the impact from other laws or regulations, misinterpretations of laws and regulations, or from a general distrust of law enforcement agencies. Some examples are included in the following discussion, and additional examples are in appendix II. We did not verify these examples.

Financial and administrative burden

Officials at the FBI, DEA, ATF, and USSS are concerned about the erosion of their investigative capabilities due to the amount of resources needed to comply with the FOI/PA requirements and the type of requesters benefiting from the acts' provisions. They said that a substantial number of staff members are processing FOI/PA requests, who could otherwise be fulfilling their investigative responsibilities. We previously reported the monetary impact of the FOI/PA on some law enforcement agencies in a report entitled "Data on Privacy Act and Freedom of Information Act Provided by Federal Law Enforcement Agencies" (LCD-78-119, June 16, 1978).

Additionally, DEA and ATF officials complained about the amount of paperwork involved in complying with the "disclosure accounting" provision of the PA. Officials of these agencies told us that when information was disclosed outside the agencies, a form indicating the information and to whom it was disseminated must be prepared. They believe this requirement has become a tremendous administrative burden which detracts from agents' time available for investigative duty.

To the Federal agencies' officials, the administrative and financial burdens seem even more destructive considering the types of individuals submitting FOI/PA requests. They believe that while these acts are of limited value to the American public, they are beneficial to criminals. According to DEA officials, about 40 percent of its requesters are prisoners asking not only for their own files but also for sensitive information, such as the agents' manual of instructions and laboratory materials describing the manufacture of dangerous drugs. An ATF official said about 50 percent of its requests come from prior offenders

APPENDIX I

APPENDIX I

who use the FOI/PA in an attempt to find out how investigations are conducted and thus avoid capture in future crimes. In our report titled "Timeliness and Completeness of FBI Responses to Requests Under Freedom of Information and Privacy Acts Have Improved" (GGD-78-51, Apr. 10, 1978), we reported that from October through December 1977 prisoners comprised about 6 percent of the requesters for information from the FBI files. In an analysis of a sample of requests submitted to the FBI, we found that 36 percent of the requests concerned criminal files.

Reduced ability to obtain information

Federal and local law enforcement officials we contacted indicated that the FOI/PA have eroded their enforcement capabilities by limiting their ability to develop investigative information from the general public, informants, and institutions.

General public

Federal and local law enforcement agencies have reported a marked reluctance of the public to cooperate with law enforcement efforts. This trend is not attributed solely to the FOI/PA. The legislation is seen as just one effect of the "post Watergate Syndrome"; that is, the public's general distrust of law enforcement agencies and the Government.

The FBI has documented numerous cases where citizens have withheld information specifically because they fear their identities will be disclosed through FOI/PA requests for information maintained by the FBI. FBI officials say these acts have eroded the public's confidence in the FBI's ability to maintain confidentiality. Citizens are reluctant to furnish derogatory information for either criminal or applicant investigations, fearing that disclosure of their testimony could result in embarrassment or civil suits against them. For example:

--A recent Department of Justice applicant investigation developed a considerable amount of derogatory information. A U.S. district judge was interviewed, and he admitted that he had information which would bear on the investigation, but he refused to furnish it to the FBI because he said he knew that his information, once released outside the FBI, would not be protected to conceal him as the source of the information. He said other Federal judges felt

APPENDIX I

APPENDIX I

the same way and believed that the Federal bench in general was unwilling to assist in such background investigations.

--In a fraud investigation in a southwestern city, a former employee of the company being investigated, who had been a principal source of information, was fearful that he would be sued by the subjects of the investigation if he provided information to the FBI. He knew this information would be available upon request under the FOI/PA, and if the criminal allegation was not ultimately resolved in court, he would become civilly liable. On several occasions this source expressed reluctance to provide information of value.

The USSS provided the following example of a citizen's reluctance to cooperate.

--In accordance with a request from the Department of Justice, USSS offices were required to make inquiries regarding the organized crime situation in their respective districts. In connection with this effort, an agent interviewed the Chief Investigator for a County District Attorney's Office, who had considerable background on organized crime activities. When interviewed, he declined to release any information. He stated that, under the FOIA, records and files of Government agencies could be obtained by non-law-enforcement personnel, that much of the information he had could not be positively substantiated, and that he could be liable for making statements he could not fully prove. He further advised that if his identity as a source of information were obtained under the FOIA, he might be subpoenaed before another body to testify on the information he had, possibly compromising his informants.

Civil Service Commission (CSC) officials, on the other hand, said that in making background investigations they have had only a minor drop in the amount of derogatory information obtained from the general public. However, they could not determine the significance of the information no longer being obtained. Actually, CSC officials were surprised at the amount of derogatory information the public provided without requiring that the information be kept confidential. CSC officials, however, expressed concern about the limits the PA imposes on collecting data

relating to how an individual exercises first amendment rights. They believe that, although this provision of the PA is not absolute, it restricts the scope of loyalty investigations and may result in some disloyal individuals entering Government service.

Informants

Federal law enforcement officials believe informants are necessary for effective criminal law enforcement, because informants are one of the most important intelligence-gathering tools. Federal officials perceive that, since the advent of FOI/PA, there has been some difficulty in recruiting and maintaining informants, especially in areas such as organized crime and foreign counterintelligence.

FBI officials believe the acts have had the greatest impact on informants in the organized crime and foreign counterintelligence areas. These individuals are usually well-educated, sophisticated, informed about the laws' provisions, and aware of recent court decisions and news articles concerning the release of information from Federal files. Informants in these areas, especially in foreign counterintelligence, are frequently respectable business people whose community standing or livelihood could be jeopardized by an FOI/PA disclosure. FBI officials said that some of these individuals are either refusing or hesitating to provide information because they believe the Government can no longer protect their identities. Sources are also concerned that if their identities are revealed they will be subject to harassment or physical retaliation. To illustrate:

--An informant connected with organized crime provided information in FBI cases, including some which led directly to the identification and prosecution of several Federal violators. Inquiring into a dramatic decrease in his productivity, the FBI learned that he became very circumspect after an organized crime figure requested and received, under the FOIA, a large volume of FBI reports and was undoubtedly trying to identify informants. The informant expects organized crime to make much greater use of the FOI/PA and doubts the FBI's ability to maintain control over the contents of its files.

--An informant who was productive for many years in the area of organized crime and

APPENDIX I

APPENDIX I

who furnished information resulting in numerous convictions became concerned that he might be identified. He indicated that newspaper accounts of FBI information disclosures under FOIA caused him to lose confidence in the FBI's ability to protect his identity. Because he had furnished information over a number of years, he believed it would be possible to identify him from a compilation of this information. The informant is presently in a position to furnish information on a major political corruption case and refuses to do so, stating that the more sensitive the information the more likely it is to "come out."

--A former source of excellent quality information was recontacted because his background was such that he could develop information of value concerning a terrorist group. He initially refused to cooperate for fear that through an FOIA disclosure his identity could eventually be revealed. He believed his information would be of such quality that anyone outside of the FBI upon reading it would easily be able to identify him. He was reminded that he had functioned as a valued source for several years and that his identity had never been disclosed. He acknowledged this was true; however, he stated that due to FOIA he no longer believes that FBI agents can assure his complete protection even though they would make every effort to do so. The source also cited recent court cases, particularly the Socialist Workers Party lawsuit, which convinced him that his identity could not be protected. After 3 hours of conversation, the former source agreed to cooperate but only in a very limited way. He made it clear he would never again function as extensively as before because of FOIA, similar laws, and court decisions. He added that disclosure of his identity would most assuredly cost him his life.

Recruiting low-level informants is less of a problem. DEA and ATF officials said the FOI/PA have had very little effect on their use of these types of informants because these individuals are involved in or on the fringes of

APPENDIX I

APPENDIX I

criminal activities and, thus, are willing to provide information in exchange for more favorable treatment of their criminal activities. Because most of them are not even aware of FOI/PA provisions, any lack of cooperation is more likely to stem from dissatisfaction about the money they have received or the deals they have made than from fear of an FOI/PA disclosure. However, FBI, DEA, and ATF officials said that, as these informants become more aware of the acts' provisions, they will be more reluctant to provide information.

FBI and ATF officials also said that, because of the FOI/PA some agents are reluctant to develop new informants. They believe they can no longer provide the 100-percent guarantee of confidentiality which is needed to avoid exposing informants to possible liability or physical harm. These officials believe their sources are vulnerable despite the acts' source-protection provisions because individuals processing FOI/PA requests do not have first-hand knowledge of the cases. Consequently, an individual processing a request may release a seemingly harmless piece of information by which the requester could identify the source.

Institutions

All law enforcement officials reported that the PA has had some of its most severe effects on their ability to obtain information from institutions such as hospitals, banks, and telephone companies. Previously, law enforcement agencies could obtain records from these institutions on an informal basis. Now, an increasing number of institutions require the agencies to obtain a subpoena before providing information.

Although the PA does not apply to private organizations, many institutions have adopted withholding information as administrative policy. Federal law enforcement officials believe these policies are a result of an increased consciousness of privacy concerns stimulated by the PA. Some organizations believe that a blanket refusal to release information without a subpoena will help protect them against invasion of privacy litigation. CSC officials said that many private companies are increasingly reluctant to allow investigators to interview employees because of PA concerns.

FBI, ATF, and USSS officials said that, in most cases, they have to use a grand jury subpoena to obtain records. This procedure is very time-consuming because of the paperwork involved and the infrequency of some grand jury meetings. FBI officials were particularly concerned over how

APPENDIX I

APPENDIX I

this procedure will affect kidnapping or fugitive cases where speed of action is essential. USSS officials said that most of the threats on the President come from mentally unstable individuals, so timely access to records maintained by mental institutions is critical when the President or other dignitaries travel around the country. Because travel schedules are sometimes not known in advance, officials cannot afford to spend considerable time trying to obtain a subpoena.

FBI, USSS, and DEA officials also said that some banks and telephone companies immediately notify the subject of the subpoena rather than allowing the customary 90-day period to elapse. Agents believe that if this immediate notification policy is continued and expanded, they will be hindered in using institutional records as investigative leads. Because organized crime and foreign counterintelligence investigations extend over long periods without the subject's knowledge, agents believe that such notifications could disclose, and thus destroy, entire investigations.

Some representative examples provided by agencies follow:

- In a case involving approximately 100 forged checks in a midwestern city, the USSS attempted to develop information on the accounts in which these checks were deposited. Banks refused to furnish copies of documents from three accounts without a subpoena, even though the banks stood to lose a total of \$40,000. These banks cited the PA as a reason for failing to furnish the requested information. Information was provided after subpoenas were served.
- During an unlawful flight to avoid prosecution/murder investigation, the FBI found out the nonpublished telephone number where the fugitive would be for the Christmas holiday. The FBI tried to obtain the location of the number from various officials of a midwestern telephone company, but they refused to release the information without a subpoena. As a result, the fugitive was not apprehended.
- In a fraud investigation the FBI was denied information submitted to Medicare through an insurance agency. This information showed Medicare fraud perpetrated by the staff of a union-owned hospital and was withheld by the

insurance agency because of the PA. Most of the information desired was ultimately obtained by a Federal grand jury subpoena.

Exchange of information affected

Federal, State, and local law enforcement officials stated that the exchange of information among law enforcement agencies has been curtailed since enactment of the PA. State privacy laws, modeled after the Federal legislation, have also limited the once free exchange of information among Federal, State, and local agencies. The information flow from non-Federal to Federal law enforcement agencies has been most affected. Foreign law enforcement agencies have expressed concern that information they provide may be disclosed through the FOIA but are still cooperating with U.S. law enforcement agencies.

Federal agencies

Federal law enforcement officials said that, in general, obtaining information from other Federal law enforcement agencies presents no serious difficulties. This is due primarily to the "routine use" provision of the PA which facilitates information flow. Under the routine use provision, Federal agencies may disclose a record for a purpose which is compatible with the purpose for which it was collected.

USSS officials were concerned about not getting as much intelligence information from the FBI as before because of restrictions imposed on the FBI's ability to collect such information. However, they cited the implementation of the Attorney General's guidelines for domestic security investigations, rather than the PA, as the reason for the reduction in the availability of information. USSS officials believe this reduction of intelligence information severely hampers its protective efforts.

FBI, DEA, and ATF officials complained about difficulties in obtaining taxpayer-related information from the Internal Revenue Service (IRS). ATF officials told us the difficulties in obtaining information from IRS arise from provisions of the Tax Reform Act of 1976 which restrict the dissemination of taxpayer-related information for non-tax related crimes.

FBI, USSS, and ATF officials indicated that gaining access to records maintained by non-law-enforcement Federal agencies has become more difficult. The FBI and USSS said that Federal agency officials often cite the FOI/PA as the

APPENDIX I

APPENDIX I

reason for withholding information. The FBI said that in many cases these officials are confused by or unaware of the disclosure provisions and requirements of the FOI/PA but are quite aware of the penalties that can be imposed for improper disclosure. Therefore, rather than risk punitive action for improper disclosures, some agency officials assume an overly conservative stance and withhold information that legally could be provided to a law enforcement agency.

Examples of cases where the FBI encountered difficulties in obtaining information from Federal agencies follow:

- FBI agents in the Pacific Northwest developed information that an escaped prisoner might have been receiving Supplemental Security Income payments. Local Social Security officials refused to supply any information about the fugitive, citing the PA. The FBI later apprehended the fugitive, after expending considerable manpower. The FBI found that the fugitive, when arrested, had been receiving Supplemental Security Income payments.
- During an FBI investigation in a western city, under the Racketeer Influenced and Corrupt Organizations statute, information developed on a subject was provided to an IRS agent. The IRS agent advised that due to the PA, the IRS could accept information valuable to them but could not provide any information that would aid an FBI-related case.
- During an unlawful flight to avoid prosecution/murder investigation, the FBI found out that the subject was receiving a monthly disability check from the Social Security Administration. Although the Social Security Administration confirmed the subject was getting a check, it declined to furnish the address where the check was being sent because of the PA. The subject was eventually located, but it took over 3 months of investigative effort.

Federal and local agencies

Most State and local law enforcement officials interviewed said they were increasingly reluctant to share intelligence information with Federal agencies because they fear that their information would be released as part of an

APPENDIX I

APPENDIX I

FOI/PA disclosure. These officials fear such disclosures will identify confidential sources or prematurely reveal investigative interests. Officials also anticipate that, in light of the current rash of lawsuits against law enforcement agencies, some subjects of investigations may eventually sue the local agencies for providing intelligence information to the Federal agencies.

Because of their concerns, most local officials said they are increasingly providing information orally and only to Federal agents with whom they have established rapport. If information is provided in writing it is "sanitized" to protect confidential information and sources. Some officials believe information exchange has become so hazardous that they could release unexpurgated data only to trusted associates who would protect its confidentiality. FBI officials corroborated the local officials' statements and provided several examples of situations in which local officials have been reluctant to provide information.

--FBI agents working on organized crime cases in a southwestern city reported that they were excluded from intelligence meetings held by State and local law enforcement agencies. Several State law enforcement officers cited concern over FOI/PA disclosures as the reason for excluding the agents from the meetings.

--A southern city's police intelligence unit learned that one of its intelligence reports, furnished to the FBI with assurances of confidentiality, had been released under the FOIA. Although this document did not reveal the identity of any informants, the unit refused to furnish any further written information to the FBI. It simply did not believe the FBI could guarantee confidentiality for information provided, and it wanted to avoid the possible compromise of informants.

--An extremist organization's leader, who was convicted of two murders, received documents from FBI headquarters through an FOIA request. The convicted leader's attorney informed a mideastern city's police intelligence officer that, after reviewing the documents, the leader had identified the police department's informant in the murder case. This police department will no longer furnish written reports to the FBI.

State privacy and access laws, modeled after the Federal legislation, also regulate dissemination of information. These laws, however, generally apply to criminal history rather than intelligence information. Under these laws, Federal law enforcement agents must now make requests in person or present documentation justifying need before the criminal history information is provided. FBI, DEA, and ATF officials said that in the past, merely a telephone call or display of credentials was sufficient to obtain the records.

CSC officials said that they have special problems in getting access to police records because some State laws do not recognize them as proper recipients of criminal history information. CSC officials believe that the difficulties stem from the fact that they are not a law enforcement agency. CSC officials also said that some local law enforcement officials mistakenly quote the Law Enforcement Assistance Administration's criminal justice information systems' regulations as requiring the withholding of information. This is done even though Law Enforcement Assistance Administration and CSC officials have explained to local officials that the regulations permit departments to release criminal history records under CSC's statutory and administrative investigative authority.

Federal and foreign agencies

Both FBI and DEA officials said that in some of their operations they depend on information provided by foreign law enforcement agencies. They also said that although these foreign agencies have continued to cooperate, they have expressed a deep concern that their information will be disclosed through the FOIA. These agencies have requested that their information always be considered confidential and thus not releasable, otherwise they would cease to provide additional information.

Although both FBI and DEA officials consider their relationship with foreign law enforcement agencies as still essentially good, they cannot tell how much information they are no longer getting because of the U.S. agencies' inability to provide total assurance of confidentiality. For example, an FBI field office reported that two officers of one prominent foreign law enforcement agency admitted they had withheld some case information from the FBI because of their concern about FOIA disclosures. During congressional testimony the Administrator of DEA cited statements by French and British officials that, if DEA were required to disclose

APPENDIX I

APPENDIX I

information furnished by them, their law enforcement agencies were certain to cease all cooperation with DEA.

AGENCY COMMENTS AND OUR EVALUATION

The Department of Justice, the Department of the Treasury, and the Civil Service Commission generally agreed with our observations. The Department of Justice, however, believes that we understated the gravity of the adverse impact the FOI/PA are having on law enforcement agencies. It also believes that we failed to emphasize the need for congressional action to remedy what it considers to be the present imbalance between the FOI/PA openness goals and the need for confidentiality in criminal and other investigations.

The benefits to the public and the difficulties experienced by law enforcement agencies resulting from the implementation of these acts cannot be quantitatively measured. The proper balance between openness and the needs of law enforcement agencies is a matter of one's perspective. Therefore we have merely presented the views of law enforcement officials and examples of how the FOI/PA are creating difficulties for law enforcement agencies. It is up to the Congress to weigh the significance of these difficulties against the public benefit derived from the openness and privacy protection provisions of the FOI/PA.

The FBI objected to our statement that "* * * no agency could document the laws' impact on overall investigative effectiveness." Officials believe that such a statement undermines the case for the Congress to reexamine the legislation. We believe that the examples provided by the FBI show that in some specific cases, it has taken the FBI longer to apprehend a criminal, that the FBI has had to spend additional agent hours collecting and/or verifying information, that the public has been increasingly reluctant to cooperate, and that some criminals are using the acts to try to obtain sensitive information from law enforcement agencies. The examples, however, do not show that the FBI or other law enforcement agencies have been unable to fulfill their investigative responsibilities.

The FBI had difficulty determining whether the impact on its operations resulted solely from the FOI/PA. Other laws or regulations, administrative policies, and a general distrust of law enforcement agencies may have had as much or more to do with the FBI's difficulties as the FOI/PA. Therefore, it was not possible to accurately document the total impact these two laws have had on the investigative operations of the FBI.

SELECTED CASE STUDIES PROVIDEDBY FEDERAL AGENCIES

Agencies we contacted almost universally agreed that law enforcement information-gathering capabilities were being eroded. They pointed out, however, that no investigative records were maintained specifically to show how these laws affect their operations. According to the FBI and USSS, the examples provided represent only the instances which could be documented after the fact and only a fraction of the total occurrences.

The FBI and USSS provided the most illustrative and specific examples, and the following sections contain a cross section of these. We did not verify the examples.

EROSION OF ABILITY TO OBTAIN INFORMATION
FROM THE GENERAL PUBLIC

- The FBI initiated a Racketeer Influenced and Corrupt Organizations investigation based on information provided by businessmen in a small southwestern town. The businessmen asked that they not be called to testify because they feared their businesses would suffer. Upon later learning that the information might be disclosed through an FOI/PA release, they decided not to furnish further information. Without this assistance the FBI had to discontinue the investigation.
- During a background investigation of a nominee for U.S. District Judge, the FBI contacted two attorneys but both were extremely reluctant to furnish their opinions of the nominee's qualifications. They feared that if the nominee was appointed and later learned of their comments, he would use his position to punish them. The attorneys had little confidence in the confidentiality protection afforded by the FOI/PA, but eventually provided some comments. However, the FBI indicated that there was no assurance that they were as candid as they might have been before passage of the FOI/PA.
- During an FBI background investigation for a possible presidential appointment, over 40 interviews were conducted and in over half of the interviews the agents believed that possible derogatory information was being

withheld. On many occasions the agents were asked if the appointee would have access to the information through the PA. Several of the individuals interviewed said that they feared reprisals and would not provide derogatory comments.

--During an FBI investigation of interstate transportation of obscene matter and interstate pimping of juvenile boys, school officials fearing reprisals if their testimony were released through the FOI/PA, refused to verify the boys' identities. Citizens in the community only reluctantly cooperated and appeared to be holding back valuable information. Several expressed fear that their identities would be revealed through an FOI/PA release. Most of the citizens indicated that organized crime was involved and feared their reputations would be damaged or their physical safety threatened. One source refused to provide any information because he did not believe the FBI could protect his identity and he feared for his life.

--An FBI office reported that the most significant negative impact on its investigative mission has resulted from a \$600,000 lawsuit filed against a person, who about 20 years ago, allegedly provided derogatory information to the FBI about the plaintiff's suitability for a Government job. The plaintiff had used the FOIA to request FBI files which she claimed allowed her to identify the source of the derogatory information. The plaintiff charged that the information was slanderous and defamatory. The suit was dismissed because the statute of limitations had run out, but the primary issue of whether or not a person can sue someone who has provided information to the FBI was never addressed or resolved. FBI agents reported that members of the general public and law enforcement officers were shocked that such a lawsuit had been filed. Numerous individuals informed FBI agents that, as a result of this lawsuit, they would never provide derogatory information to the FBI.

APPENDIX II

APPENDIX II

- In an FBI applicant investigation a local police official refused to provide derogatory information concerning the applicant. The official said that under the FOIA the applicant would have access to the information and, even if his identity were to remain confidential, the information could serve to identify him.
- FBI agents contacted the former employer of a person applying for an FBI position. Company officials provided the dates of employment, but refused to provide a recommendation or comment on the employee's performance, citing the PA and the fact that the information could become known to the applicant. The officials further stated that no other information would be provided regarding the applicant, even if the applicant signed a release form.
- The FBI was investigating the financial status of a person convicted of fraud against the Government. This individual had consented to a \$300,000 judgment. A potential Government witness refused to furnish information regarding ownership and management of the defendant's property after being advised about the FOIA's provisions. The potential witness believed that an FOIA release would adversely affect his business relations with the defendant.

EROSION OF ABILITY TO RECRUIT AND/OR
MAINTAIN INFORMANTS

- A top management official in a State agency wanted to provide the FBI with information on white collar crime and political corruption. However, he refused to provide the information because he doubted the FBI could protect his identity due to the access possible through the FOIA.
- A potential counterintelligence source advised that he could not cooperate with the FBI because he feared that his identity would be revealed publicly. He indicated that recent newspaper accounts regarding material released under the FOIA had revealed the names of several individuals in a professional capacity who had assisted the FBI, and the nature of their

APPENDIX II

APPENDIX II

assistance. This type of publicity, according to the individual, would be detrimental to any person in business who elected to cooperate with the FBI.

- An FBI informant who had regularly furnished information resulting in recovery of large amounts of stolen Government property, arrests, and convictions, relocated and discontinued his services. Upon his return to a position where he could furnish similar information, he refused to cooperate because he feared that through an FOI/PA release he would be identified and his life would be jeopardized.
- A businessman was approached by an intelligence officer from a hostile country. During an FBI interview, the businessman said that were it not for the FOI/PA he would be willing to cooperate with the FBI in foreign counterintelligence involving the intelligence officer who contacted him plus any others. He refused to get involved because he feared that his identity would be divulged, thus seriously affecting his business operations.
- A source providing foreign counterintelligence information expressed anxiety on numerous occasions about continuing his relationship with the FBI. He fears that his identity will be disclosed through an FOI/PA release, thus hurting his business and jeopardizing members of his family who reside inside the hostile country. Because of his fears the source frequently requests the FBI to place dissemination restrictions on the information he furnishes.
- In a southwestern city, an individual who is in a position to furnish foreign counterintelligence information has refused to cooperate. It is his opinion that the Federal Government cannot insure his confidentiality in view of congressional scrutiny of the FBI, subsequent news media leaks, access to records through the FOI/PA and the extensive civil discovery proceedings exemplified by the Socialist Workers Party lawsuit, where the court has ordered the Government to disclose the identity of some informants. The individual said that if the disclosure climate was more restrictive he would be willing to cooperate.

- An FBI informant, who provided information regarding gambling and organized crime in a southern city, asked to terminate his FBI association because he believed that the FBI could not sufficiently protect his identity. The source is afraid that his identity may be revealed under the FOI/PA causing him to lose his business.
- In June 1978, an FBI agent from a southwestern city met with a source to seek help in locating a wanted person. The source said that he did not want to continue providing information and would not help. The source believed that the FBI could no longer guarantee confidentiality in light of the FOI/PA and recent court cases such as the Socialist Workers Party lawsuit.
- During an investigation to locate an armed robbery fugitive, the local police developed an informant close to the fugitive. The informant initially provided valuable information, but upon realizing that the local police were sharing the information with the FBI the informant refused to continue cooperating, believing that her identity might be revealed through an information request under the FOI/PA. The fugitive committed several crimes during the additional time that was required to apprehend him.

EROSION OF ABILITY TO OBTAIN INFORMATION
FROM NON-GOVERNMENTAL INSTITUTIONS

- A forged U.S. Treasury check was used to pay a telephone bill. The telephone company supervisor refused to furnish USSS agents with any information about the individual who negotiated the check or the telephone account involved. Although the USSS agent pointed out that the telephone company was a victim in this case, the company refused to furnish any data without a court order. The Secret Service agent said that this information would not have been withheld prior to enactment of the FOI/PA.
- A USSS agent, working undercover, learned that a \$3,800 U.S. Treasury check had been stolen, forged, and deposited in a bank account in a west coast city. The Secret Service immediately called all the banks in the city, with negative

APPENDIX II

APPENDIX II

results. The undercover agent later learned which bank had received the check. When he visited this bank, bank officials acknowledged they had been contacted earlier, but had ignored the inquiry because it was bank policy not to reply to law enforcement inquiries because of the PA. By the time the agent made the initial telephone call to the bank, \$500 had been withdrawn from the account. The subjects withdrew an additional \$2,500 between the initial call and the visit by the Secret Service agent. The bank would have prevented a \$2,500 loss if it had cooperated when first contacted.

--A west coast bank advised the FBI that the bank had made a \$100,000 loan to an individual who appeared to have provided false information on the loan application. The bank indicated that this person may also have defrauded several other banks. The FBI contacted the bank official who had the loan records but he refused to release the documents without a subpoena. The FBI then contacted the assistant U.S. attorney who advised that he would not issue a subpoena without knowing what information of evidential value was contained in the records. Because of this "Catch-22" situation, the FBI closed the investigation. The case was eventually reopened in light of the amount of losses suffered (several million dollars).

--In a fugitive-deserter investigation the FBI found out that the subject had worked at a particular oil company. The oil company was contacted but refused to provide the subject's address or other background information. The company feared future liability if the subject learned that the company provided the information to the FBI. Company officials believed the FBI would have to provide this information to the subject because of the FOI/PA.

--During an FBI fugitive investigation of a subject wanted for extortion and firearms violations, an agent contacted a hotel's security officer to develop background information on a former employee who was an associate of the fugitive. This former employee allegedly had knowledge of the fugitive's whereabouts, but the security officer refused to provide any information from the files without a

subpoena. The security officer believed that without a subpoena the hotel would be subject to civil litigation under provisions of the PA.

- A west coast telephone company informed the USSS that whenever the company releases information about a non-published number, they will immediately notify the subscriber that an inquiry was made and who made the inquiry. Consequently, agents must now decide whether to obtain the information and thus alert the subscriber, or not use this important investigative tool.
- During a sensitive investigation, the FBI subpoenaed bank records concerning the subject of the investigation. Contrary to a prior agreed upon arrangement, the bank manager immediately advised the subject that the FBI had requested the records and jeopardized several ongoing investigations. The manager justified his action by citing the PA. As a result of this experience, agents working on another sensitive investigation decided not to request needed bank records because the risk of the bank notifying the suspect was too great.

EROSION OF ABILITY TO EXCHANGE INFORMATION
WITH OTHER FEDERAL AGENCIES

- An FBI office in the South reported that FBI agents must now obtain change of address information from the Postal Inspector's Office. Previously, FBI agents with proper identification could get this information from the local postal substation. Furthermore, the Postal Service asked this FBI office not to contact individual mail carriers for information. The mail carriers, who are familiar with neighborhood activity, are considered valuable sources to whom access is now denied.
- A father took his 5-year old son away from the boy's grandfather who had legal custody. As a result, a Federal warrant was filed for the father's arrest and the FBI began looking for him. Three months later, the father contacted the Social Security office in the city where the child previously lived and requested that the child's Social Security check be forwarded to another office. The Social Security office told

the grandfather about the request. The FBI immediately contacted the Social Security claim representative, explained that there was a Federal warrant for the father's arrest and asked where the father wanted the check sent. The claim representative told the FBI that Social Security headquarters had instructed him not to release any information without a subpoena. Two days later, the assistant U.S. attorney obtained a subpoena from the U.S. District Court Clerk and the FBI served the claim representative with the subpoena. Local Social Security officials contacted the Assistant Regional Attorney of the Department of Health, Education, and Welfare, who advised them not to honor the subpoena based on Social Security regulations. The assistant U.S. attorney then advised the grandfather to go to the local Social Security office and request the needed information under the FOIA. Through an FOIA request, the grandfather received all the information needed to enable the FBI to locate the child and arrest the father.

- In a recent USSS stolen check investigation, three empty Government check envelopes were found in the suspect's bedroom. Each envelope had apparently been used by the suspect to practice writing the payee's name. Two of the written names were identified and the payees were located. The third name could not be identified and an inquiry was made at the local Social Security office to determine if checks were being issued in this name. Social Security office personnel cited the PA and refused to provide any information. Copies of the forged check were subsequently obtained through formal channels 6 months later.

- In an eastern city, the FBI received information from the State police concerning possible fraud. An individual was allegedly receiving full Social Security disability payments, while still working full time. The FBI contacted the local Social Security office, but the office chief refused to provide any information, including whether or not the individual was receiving disability payments. The official cited the provisions of the FOI/PA as the reason for not giving the information.

--On a large military installation, FBI agents were investigating the theft of lumber and needed to interview persons working in the installation's electrical generating plant over the weekend. The officer in charge declined to furnish the weekend work schedule because of the PA. The FBI had to obtain the assistance of a Judge Advocate General officer before the list was made available.

EROSION OF ABILITY TO EXCHANGE INFORMATION
WITH STATE AND LOCAL LAW ENFORCEMENT AGENCIES

- A midwestern State's police intelligence unit advised that the unit's officers will provide information only to Federal agents who they know personally. Their rationale is that they can trust the agents they know to properly conceal informant identities even if the information is later released under the FOI/PA.
- The FBI learned that an FBI applicant was a former employee of a midwestern State's bureau of investigation. When contacted, State bureau officials acknowledged they had derogatory information concerning the applicant but refused to reveal the information because the applicant would have access to it under the PA.
- During a suitability investigation of a political appointee, the officer in charge of a police department's organized crime bureau advised the FBI that he had furnished derogatory information about the appointee directly to the congressional committee which had requested the FBI investigation. He added that the derogatory information concerned national security, but refused to comment further. The officer later told the FBI that he was thoroughly familiar with the confidentiality provisions of the FOI/PA, but was also aware that the legislation is subject to interpretation. Consequently, he refused to give the derogatory information to the FBI. After receiving this derogatory information, the committee refused to provide this information to the FBI and requested the FBI to discontinue its investigation.
- In a southwestern State, a member of a local law enforcement agency told the FBI that while

APPENDIX II

APPENDIX II

police reports and other verified data would be disseminated, the agency would be reluctant to provide intelligence data because of the possible release under the FOI/PA.

--In an eastern city, the FBI reported that local police officers are reluctant to make all information available concerning subjects of investigations because of the FOI/PA. The police department has told the FBI that if one of its sources is exposed through an FOI/PA release, it will no longer make its records available to the FBI, even on a personal basis.

SUMMARIES OF THE
FREEDOM OF INFORMATION ACT
AND PRIVACY ACT

THE FREEDOM OF INFORMATION ACT

The Freedom of Information Act, ^{1/} signed into law on July 4, 1966, directs that all Federal executive branch agencies' records must be made available to the public, except information specifically exempted by the act. The law provided new disclosure standards and practices to be applied by the executive agencies. The law, which was meant to improve public access to information held by Federal agencies, established a judicial review of agency actions. This review makes it necessary for agencies to justify the withholding of information.

The act identifies nine categories of information that can be exempt from release. These categories are (1) information classified pursuant to executive order, (2) information related solely to an agency's internal rules and practices, (3) information specifically exempted from disclosure by statute, (4) trade secrets and confidential commercial or financial information, (5) agency memorandums that would not be available by law, (6) files whose disclosure would constitute a clearly unwarranted invasion of privacy, (7) investigatory records compiled for law enforcement purposes, (8) certain information related to regulation or supervision of financial institutions, and (9) geological and geophysical data. However, the act's legislative history makes it clear that the Congress did not intend for agencies to use these exempt categories to automatically withhold information.

The FOIA amendments, passed by the Congress in 1974 and effective February 19, 1975, were designed to

- limit the Government's authority to withhold certain kinds of information,
- strengthen the public's right to obtain information from Federal records, and
- speed public access to Federal Government records.

THE PRIVACY ACT

The Privacy Act 1/ was enacted on December 31, 1974. This act emphasizes protecting an individual's personal privacy and provides an individual the opportunity to review, and obtain a copy of his or her record maintained by a Federal agency. The PA provides for exemptions which, like the FOIA's, are permissive not mandatory. Unlike those of the FOIA, the PA's exemptions apply to systems of records rather than to requests for access to specific information.

The PA also allows individuals to request that their records be amended and that records they believe inaccurate be corrected or deleted. If the agency either denies access or refuses to amend a record, the PA allows for judicial review of the agency's action. The court may assess against the Government reasonable attorney fees, as well as award damages to the individual, if the requester substantially prevails.

Among the administrative requirements involving the collection, maintenance, use, and dissemination of an agency's records, the PA requires that each agency publish annually in the Federal Register

- a descriptive list of its records systems and
- the procedures to enable people to obtain their own files.

1/5 U.S.C. 522a

APPENDIX IV

APPENDIX IV



UNITED STATES CIVIL SERVICE COMMISSION

WASHINGTON, D.C. 20415

SEP 13 1978

IN REPLY PLEASE REFER TO

YOUR REFERENCE

Mr. H. L. Krieger
 Director, Federal Personnel and
 Compensation Division
 U.S. General Accounting Office
 Washington, D.C. 20548

Dear Mr. Krieger:

These are our comments on your draft report entitled "Erosion of Law Enforcement Capabilities Attributed to the Freedom of Information and Privacy Acts."

As an initial matter, we should point out that some of the difficulty agencies with law enforcement functions are experiencing with the Privacy Act results from an interpretation of certain provisions of the Act in the case of Gang v. United States Civil Service Commission, et al., Civ. No. 76-1263 (D.D.C. 1977). A copy of that decision is attached to this letter for your information.

In the Gang case, the court held that the Civil Service Commission violated subsection (e)(6) of the Act by failing to make "reasonable efforts" to assure that an investigative file furnished to the Library of Congress on the plaintiff was accurate, complete, timely, and relevant for agency purposes. This is required by the Act when a file is disseminated to someone "other than an agency". The court found the Library of Congress was not an "agency" for purposes of this provision since it is an instrumentality of the legislative, rather than the executive, branch of the Federal Government. This conclusion was drawn despite a longstanding agreement between the Library of Congress and the Commission that the former would be treated as an agency for purposes of receiving Commission investigative files.

As a result, all agencies furnishing investigative files to other than executive branch agencies (for example, GAO) must attempt to screen the files to satisfy the amorphous standard of accuracy, relevance, timeliness and completeness or assume the risk of violating this provision of the Act.

THE MERIT SYSTEM—A GOOD INVESTMENT IN GOOD GOVERNMENT

APPENDIX IV

APPENDIX IV

Moreover, the court found that the Commission violated subsection (e)(7) of the Act by maintaining information on how the plaintiff had exercised First Amendment rights. Agencies are permitted to maintain information of this character only if it is "expressly authorized by statute, or by the individual about whom the record is maintained or unless pertinent to and within the scope of authorized law enforcement activity." However, the court found that the background security investigation conducted by the Commission was not a "law enforcement activity" despite a clear reference in the legislative history of the Act to the effect that background investigations should be regarded as a law enforcement activity.

While this one decision may not be absolutely dispositive of this issue, it has undoubtedly resulted in a wariness on the part of agencies conducting security or suitability background investigations about collecting information that may conceivably be regarded as an exercise of First Amendment rights.

Perhaps the most significant impact on agency law enforcement activities, however, has come at the collection stage even though, as you point out in your draft report, the Commission continues to receive good cooperation generally from the public in obtaining derogatory information. The Office of Administrative Law Judges of the Commission which examines administrative law judge applicants has cited a number of instances of non-cooperation by potential sources of information because of Privacy Act access by the subject of the inquiry. Copies of material manifesting non-cooperation by sources are attached to this letter for your information. In addition, that Office feels that Privacy Act access has caused sources who do cooperate to be less candid and frank in their evaluations.

(See GAO note, p. 36.)

APPENDIX IV

APPENDIX IV

(See GAO note, p. 36.)

We hope you find these comments helpful in preparing the final version of your report.

Sincerely yours,


Raymond Jacobson
Executive Director

Enclosure

APPENDIX V

APPENDIX V



ASSISTANT SECRETARY

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OCT 5 1978

Dear Mr. Lowe:

This responds to your letter of August 23, 1978, requesting our comments on the United States General Accounting Office draft report entitled, "Erosion of Law Enforcement Capabilities Attributed to the Freedom of Information and Privacy Acts."

The report accurately reflects the many concerns and difficulties experienced by Treasury Department law enforcement agencies since the enactment of the Freedom of Information and Privacy Acts.

The Treasury Department is well aware of the public and legislative concerns which led to the enactment of these statutes. We are sympathetic to these concerns, and have established procedures to assure timely responses to public requests made under the provisions of these acts.

However, we have found that compliance with the Freedom of Information Act places two burdens upon our law enforcement activities. First, some resources must be diverted from other operations to handle the review and editing of materials requested by the public. Second, there has been some diminution in the flow of information provided to Treasury law enforcement agencies from what heretofore have been vital sources, such as, State, local and foreign law enforcement agencies, public utilities, educational institutions, and confidential informants. Our law enforcement agencies are unable, however, to provide a precise quantification of the extent of this diminution.

The reluctance to voluntarily release information to Treasury law enforcement agencies is based upon a concern by the sources of information that Freedom of Information Act inquiries may lead to public disclosure of information provided by them which previously had been considered confidential. Confidential informants are particularly

concerned that their identity may be revealed through such disclosures either by direct disclosure, or indirectly, based upon other information which has been released. These laws have also adversely affected the gathering of information from the business community. For example, the Customs Service which enforces the statutes governing fraud, antidumping, countervailing duties, and classification and appraisement of imported merchandise has found it difficult to obtain commercial information for enforcement of these statutes without the use of subpoenas.

While the diversion of staff resources to process Freedom of Information Act and Privacy Act requests clearly has a negative impact on our law enforcement capabilities, this direct reduction does not represent the only effect of these statutes upon law enforcement. There are other significant but intangible costs of processing Freedom of Information Act requests. For instance, when a request is made for an open investigative file, the steps necessary to process that request will tend to disrupt the investigation. Records in open cases are generally exempt from disclosure under the Freedom of Information Act. However, the tasks of locating, indexing, and defending the records from disclosure under the Act can complicate law enforcement activity. Enforcement personnel must be diverted from their investigative activities to spend time analyzing the releasability of material in the investigative file, and the file itself becomes temporarily unavailable for the purpose for which it is maintained.

We have found that the 1974 Amendments to the Freedom of Information Act have, as expected, greatly decreased our ability to protect the confidentiality of our sources of information. Prior to the 1974 Amendments, the scope of the exemption for investigatory material was of a broader nature. Specifically, it provided that its disclosure dictates were not applicable to "investigatory files compiled for law enforcement purposes except to the extent available by law to a private party." However, the 1974 Amendments made investigatory materials more readily available to public access. Now, as a general rule, investigatory material can be protected only if its disclosure would 1) interfere with a concrete prospective enforcement proceeding, 2) prejudice a person's right to a fair trial or impartial adjudication, 3) cause an unwarranted invasion of personal privacy, 4) disclose the identity of a confidential source, 5) disclose investigative techniques, or 6) endanger the life or physical safety of law enforcement personnel.

APPENDIX V

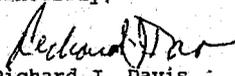
APPENDIX V

One of the effects of this Amendment has been to offer to subjects of criminal investigations a viable alternative to the discovery procedures available in each of the various judicial forums. The structure of the Freedom of Information Act, particularly with respect to the manner in which litigation is to be conducted, encourages court tests of agency decisions to withhold information regardless of the obvious applicability of the claimed exemption. The burden of proof in any Freedom of Information Act suit is upon the defendant agency, and the judicially recognized methods of sustaining this burden in many instances afford the plaintiff at least indirect relief. In this regard, it has become commonplace for courts to require agencies to submit detailed affidavits regarding the claimed exemptions and/or indices of the documents or portions thereof with respect to which exemption claims have been asserted in conjunction with motions for summary judgment. Should large numbers of individuals who are subject to pending criminal proceedings institute actions of this type, the Department would find it extremely difficult to meet the increased workload requirements.

While it is recognized that individuals have a right to obtain relevant information maintained by the government, it must also be recognized that these laws have had an adverse impact on the ability of Treasury law enforcement bureaus to perform their missions effectively. I firmly believe it is necessary to find a middle ground where the rights of individuals to privacy and open Government as well as to effective law enforcement are protected.

Please contact me if I may be of any further assistance in the matter.

Sincerely,


Richard J. Davis
Assistant Secretary
(Enforcement and Operations)

Mr. Victor L. Lowe
Director
General Government Division
U. S. General Accounting Office
Washington, D. C. 20548

APPENDIX VI

APPENDIX VI



UNITED STATES DEPARTMENT OF JUSTICE

WASHINGTON, D.C. 20530

Address Reply to the
Division Indicated
and Refer to Initials and Number

OCT 26 1978

Mr. Allen R. Voss
Director
General Government Division
United States General Accounting Office
Washington, D.C. 20548

Dear Mr. Voss:

This letter is in response to your request for comments on the draft report entitled "Erosion of Law Enforcement Capabilities Attributed to the Freedom of Information and Privacy Acts."

It is clear from our reading of the draft report that the Freedom of Information and Privacy Acts (FOI/PA), as perceived by law enforcement officials and informants, have resulted in an erosion of investigative information. There is a pervasive, widely held, and deeply felt conviction that the FOI/PA are having an unforeseen adverse impact upon law enforcement. Our concern, however, is that the report, as written, fails to highlight this perception and its crippling impact upon the Department's investigative work, primarily with regard to the Federal Bureau of Investigation and the Drug Enforcement Administration.

An appropriate balance must be struck between the salutary goals of the FOI/PA and the equally important necessity of protecting confidentiality in criminal and other investigations. We are convinced that there is now sufficient evidence to justify a congressional reexamination of this balance. This aspect of the report needs to be more strongly emphasized.

Federal Bureau of Investigation (FBI)

The FBI expended considerable effort to document, by example, the erosive consequences of the FOI/PA legislation and to facilitate numerous interviews by GAO personnel of special agents conducting investigations in the field and supervisory personnel at FBI Headquarters. Numerous examples were submitted by the FBI from virtually every field office in each of the categories for GAO's review. Selections of the information included in the report demonstrate (1) diminished public cooperation, (2) diminished law enforcement exchanges of information, (3) diminished informant assistance, and (4) other adverse ramifications.

The examples furnished clearly indicate the FBI is not now receiving vital information previously provided by the public, private institutions, Federal agencies, informants and foreign, State and local law enforcement organizations. Some investigations had to be discontinued altogether. Other investigations required many additional man-hours to resolve, and during these extended periods some fugitives remained at large committing additional crimes which could have been prevented. As the report clearly depicts, elements of organized crime and other criminal groups are using the FOI/PA statutes to determine the method and extent of the Government's penetration of their activities and to identify informants.

Although GAO went to considerable length to obtain examples and present them in an objective manner, the report suggests on page 4 of Appendix I that ". . . no agency could document the laws' impact on overall investigative effectiveness." We think this statement undermines the case for reexamination.

Drug Enforcement Administration (DEA)

While the right to access to information by the criminal element is legitimate under provisions of the FOI/PA, it nevertheless is a significant detriment to the effective operation of DEA's criminal investigatory activities. It impacts on virtually every aspect of investigative activity and creates a restrictive climate in a number of areas. The impact in the more significant areas includes:

GAO note: Page reference in this appendix refers to the draft report and does not necessarily agree with the page number in this report.

- It diminishes the ability to obtain cooperation and information from individuals, businesses and institutions.
- It hampers efforts to recruit and maintain informants.
- It impedes the free exchange of drug-related information with foreign, State and local law enforcement organizations.

(See GAO note, p. 36.)

One area of special concern to DEA involves the use of information disseminated via the FOI/PA to members of criminal organizations. These organizations attempt to manipulate the criminal justice system and thus abort investigative efforts concerning their activities. The U.S. Senate, Permanent Sub-Committee on Investigations, held hearings on August 10, 1978, dealing with aspects of criminal misuse of the FOI/PA. The hearing dealt with testimony by a convicted criminal, Gary Bowdach, and, in our opinion, clearly established the laws' impact on diminishing our overall investigative effectiveness. Mr. Bowdach made statements to the Sub-Committee that the criminal element goes beyond their legal rights in that they use FOI/PA requests to "bog down the system, tie up law enforcement personnel, prosecutors." They use the acts to "subvert the criminal justice system," and to "assassinate people that are cooperating with the government."

Although DEA is powerless to completely prevent these manipulative efforts by the criminal element, we consider it our duty to make sure that those who interpret the FOI/PA recognize these facts so that they may be appropriately guided to interpreting the law in the spirit in which intended.

APPENDIX VI

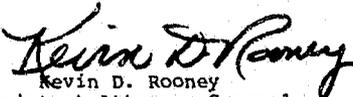
APPENDIX VI

Financially and administratively the FOI/PA are very expensive to administer and impose both stringent procedural and heavy proof burdens on the recipient bureaus. The burden is made doubly severe when the bureaus feel compelled to bring teams of agents in from the field to process the backlog of FOI/PA requests. The FBI and DEA have both felt it necessary to resort to such temporary remedies, resulting in the loss of valuable workyears in field investigations. In recent years the bureaus have requested increased funding in order to cope with the escalating demand for records to be made available through the FOI/PA. However, because of the extreme scarcity of resources, we have been hesitant to approve increases or reprogram current resources when the extent of the long-run demand for FOI/PA materials in the future is, at best, conjectural.

A major concern of both FBI and DEA continues to be the problem of meeting the policies of FOI/PA, the courts and the Department, and yet be assured that confidential source information is adequately protected. It is often difficult to prevent disclosure of precisely the information which risks exposure of informants and/or reveals the scope and penetration of the investigation of organized crime elements. It is important to recognize that diminished effectiveness is difficult to measure, given the many factors present in any investigative program. Our concern for the future is the striking of a just balance between the public's legitimate access to information and law enforcement's need to protect information essential to successful pursuit of investigations.

We appreciate the opportunity to comment on the draft report. Should you desire any additional information, please feel free to contact us.

Sincerely,


Kevin D. Rooney
Assistant Attorney General
for Administration

GAO note: Deleted comments refer to material contained in our draft report which has been revised or to material which has not been included in the final report.

(18436)

END