WIRETAPPING AND ELECTRONIC SURVEILLANCE

HEARINGS

BEFORE THE

SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES, AND THE ADMINISTRATION OF JUSTICE

OF THE

COMMITTEE ON THE JUDICIARY HOUSE OF REPRESENTATIVES

NINETY-THIRD CONGRESS

SECOND SESSION

ON

H.R. 1597, H.R. 7773, H.R. 9781, H.R. 9815, H.R. 9973, H.R. 10008, H.R. 10331, H.R. 11629, H.R. 11836, and H.R. 13825

RELATING TO WIRETAPPING AND ELECTRONIC SURVEILLANCE

APRIL 24, 26, AND 29, 1974

Serial No. 41

Printed for the use of the Committee on the Judiciary

WIRETAPPING AND ELECTRONIC SURVEILLANCE

HEARINGS

BEFORE THE

SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES, AND THE ADMINISTRATION OF JUSTICE

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

NINETY-THIRD CONGRESS

SECOND SESSION

ON

H.R. 1597, H.R. 7773, H.R. 9781, H.R. 9815, H.R. 9973, H.R.10008, H.R. 10331, H.R. 11629, H.R. 11836, and H.R. 13825

RELATING TO WIRETAPPING AND ELECTRONIC SURVEILLANCE

APRIL 24, 26, AND 29, 1974

Serial No. 41

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

35-391 WASHINGTON : 1974

COMMITTEE ON THE JUDICIARY

PETER W. RODINO, JR., New Jersey, *Chairman*

HAROLD D. DONOHUE, Massachusetts
JACK BROOKS, Texas
ROBERT W. KASTENMEIER, Wisconsin
DON EDWARDS, California
WILLIAM L. HUNGATE, Missouri
JOHN CONYERS, JR., Michigan
JOSHUA EILBERG, Pennsylvania
JEROME R. WALDIE, California
WALTER FLOWERS, Alabama
JAMES R. MANN, South Carolina
PAUL S. SARBANES, Maryland
JOHN F. SEIBERLING, Ohio
GEORGE E. DANIELSON, California
ROBERT F. DRINAN, Massachusetts
CHARLES B. RANGEL, New York
BARBARA JORDAN, Texas
RAY THORNTON, Arkansas
ELIZABETH HOLTZMAN, New York
WAYNE OWENS, Utah
EDWARD MEZVINSKY, Iowa

EDWARD HUTCHINSON, Michigan
ROBERT McCLORY, Illinois
HENRY P. SMITH III, New York
CHARLES W. SANDMAN, JR., New Jersey
TOM RAILSBACK, Illinois
CHARLES E. WIGGINS, California
DAVID W. DENNIS, Indiana
HAMILTON FISH, JR., New York
WILEY MAYNE, Iowa
LAWRENCE J. HOGAN, Maryland
M. CALDWELL BUTLER, Virginia
WILLIAM S. COHEN, Maine
TRENT LOTT, Mississippi
HAROLD V. FROEHLICH, Wisconsin
CARLOS J. MOORHEAD, California
JOSEPH J. MARAZITI, New Jersey
DELBERT L. LATTA, Ohio

JEROME M. ZEIFMAN, *General Counsel*
GARNER J. CLINE, *Associate General Counsel*
HERBERT FUCHS, *Counsel*
HERBERT E. HOFFMAN, *Counsel*
WILLIAM P. SHATTUCK, *Counsel*
H. CHRISTOPHER NOLDE, *Counsel*
ALAN A. PARKER, *Counsel*
JAMES F. FALCO, *Counsel*
MAURICE A. BARBOZA, *Counsel*
FRANKLIN G. POLK, *Counsel*
THOMAS E. MOONEY, *Counsel*
MICHAEL W. BLOMMER, *Counsel*
ALEXANDER B. COOK, *Counsel*
CONSTANTINE J. GEKAS, *Counsel*
ALAN F. COFFEY, JR., *Counsel*

SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES, AND THE ADMINISTRATION OF JUSTICE

ROBERT W. KASTENMEIER, Wisconsin, *Chairman*

GEORGE E. DANIELSON, California
ROBERT F. DRINAN, Massachusetts
WAYNE OWENS, Utah
EDWARD MEZVINSKY, Iowa

TOM RAILSBACK, Illinois
HENRY P. SMITH III, New York
CHARLES W. SANDMAN, JR., New Jersey
WILLIAM S. COHEN, Maine

HERBERT FUCHS, *Counsel*
WILLIAM P. DIXON, *Counsel*
BRUCE A. LEHMAN, *Counsel*
THOMAS E. MOONEY, *Associate Counsel*

CONTENTS

WIRETAPPING AND ELECTRONIC SURVEILLANCE

WEDNESDAY, APRIL 24, 1974

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES,
AND THE ADMINISTRATION OF JUSTICE OF THE
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The subcommittee met at 10 a.m., pursuant to call, in room 2141, Rayburn House Office Building, Hon. Robert W. Kastenmeier (chairman) presiding.

Present: Representatives Kastenmeier (presiding), Danielson, Drinan, Mezvinsky, Railsback, Smith, and Cohen.

Also Present: Bruce A. Lehman, counsel, and Thomas E. Mooney, associate counsel.

Mr. KASTENMEIER. The subcommittee will come to order.

Other members of the subcommittee will be joining us shortly. The Chair would like to make a statement relative to the hearing which we have before us today.

Privacy is an essential element in the American ideal of liberty, a basic right recognized by the fourth amendment to the Constitution. As Justice Brandeis wrote, each individual's right to privacy is "the most comprehensive of rights, and the right most valued by civilized men."

Within the last several years many citizens have begun to fear that this basic right is being steadily eroded by the use of modern electronic technology to eavesdrop on conversations. Unfortunately, increasing numbers of Americans have begun to fear that Government is more interested in intruding into their private lives than in acting to protect their privacy. A basic purpose of these hearings is to examine the trend toward privacy invasion and to determine what should be done to reassert the right of the individual to be free of Government surveillance.

Until passage of the Omnibus Crime Control and Safe Streets Act of 1968, the only Federal statute on wiretapping was section 605 of the Federal Communications Act of 1934, which prohibited interception and divulgence of conversations transmitted by wire. The Department of Justice interpreted section 605 to mean that the law was violated only if an intercepted conversion was divulged to outsiders, and the question was never decided by the Supreme Court. It was not until the 1968 act that Congress enacted a comprehensive statute on wiretapping and electronic surveillance.

That statute, title III of the Omnibus Crime Control and Safe Streets Act, actually extended official wiretapping by authorizing frequent and prolonged eavesdropping by Federal and State investigators. It also authorized, for the first time, the use of wiretap evidence in criminal trials. In the 6 years since the enactment of title III we have witnessed an intensive, widespread, but perhaps avoidable encroachment on some of our most necessary rights.

These hearings are not the first congressional effort to examine privacy invasion by electronic eavesdropping. Between 1934 and 1967 at least 16 sets of congressional hearings on wiretapping were held. From 1965 to 1971 former Congressman Corneillius Gallagher conducted numerous hearings on privacy invasion as chairman of the Special Subcommittee on Privacy of the House Committee on Government Operations. However, in 1972 the House defeated a resolution sponsored by Congressman Gallagher to establish a Select Committee on Privacy, Human Values, and Democratic Institutions. The then chairman of the Judiciary Committee, Congressman Celler took the position that the entire subject of privacy was within the jurisdiction of this committee even though Congressman Gallagher tried without success to assure Chairman Celler that the proposed select committee would not encroach on the Judiciary Committee's recognized jurisdiction in the area of bugging, wiretapping, and surveillance.

In scheduling these hearings this subcommittee is reasserting the Judiciary Committee's longstanding involvement with the problems of privacy invasion and electronic surveillance.

Of course, we are not alone in our examination of this sensitive subject. Within the last few weeks, two subcommittees of the Senate Judiciary Committee and one subcommittee of the Senate Foreign Relations Committee have begun joint hearings on warrantless wiretapping and electronic surveillance.

In addition, there are two independent commissions which are authorized to consider the problem. Public Law 90–351 established a National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. Recently, Congressman Railsback of this subcommittee and I were appointed as two of the House Members on this Commission. Congressman Edwards of California and Congressman Steiger of Arizona are the other House Members.

Public Law 91–452 established another Commission, the National Commission on Individual Rights, which also has a mandate to consider wiretapping and electronic surveillance. I am also a member of that Commission. Unfortunately, this Commission cannot function presently as the President has failed to appoint its public members.

Undoubtedly, these two Commissions will serve a useful purpose in undertaking a full scale reappraisal of the problem of privacy invasion by electronic eavesdropping. However, the growing public concern in this area requires that we not wait for the result of the Commission's findings to exercise our oversight in this sensitive area.

Within the last year numerous reports have appeared in the press describing abuses of wiretapping and electronic surveillance on the

part of the Federal Government. Only last week this issue of illegal Government wiretapping was raised in a Federal court in Minnesota in prosecutions arising out of the incident at Wounded Knee. Recent testimony before the Senate Judiciary Subcommittee on Constitutional Rights revealed that U.S. military intelligence units had tapped telephones of American citizens living in Europe who were organized to support Senator George McGovern's 1972 campaign for the Presidency. In addition, there have been numerous reports of wiretapping of members of the press, advisors to Presidential candidates and even members of Congress. These reports emphasize the need for immediate Subcommittee consideration of Government eavesdropping activities.

The procedures used within the Department of Justice to approve wiretapping requests have also been questioned. In litigation presently pending before the Supreme Court, the Justice Department has admitted that former Attorney General John Mitchell's executive assistant actually reviewed and signed wiretap requests in spite of the fact that the law requires that such requests be signed by the Attorney General or a designated Assistant Attorney General. This failure by the Attorney General to observe the law could compromise hundreds of prosecutions of organized crime figures who were wiretapped under such procedures.

That reported abuses of wiretapping and electronic surveillance have generated public concern is reflected by the fact that over 30 members of Congress have sponsored legislation which would restrict currently authorized eavesdropping. This legislation is currently pending before this subcommittee.

In view of the public and congressional concern about eavesdropping, the subcommittee has an obligation to find out the facts about this much publicized subject. Hopefully, these hearings will provide some of those facts. I feel very strongly that the all-too-clever techniques of modern electronic eavesdropping require the vigilance of the Congress to protect the right of the individual. This most insidious invasion of privacy demands full recognition and certain action.

We must also recognize the needs of investigative agencies for the best techniques available in the fight against organized crime and in the protection of our national security. I think that most citizens want our law enforcement agencies to be well equipped to perform their investigative responsibilities within the limitations imposed by the Constitution.

We will be hearing from a variety of witnesses representing both those who have been under surveillance and those who have conducted surveillance.

[The bills are as follows:]

[H. R. 1597, 93d Cong., 1st sess.]

A BILL To amend certain Federal law relating to the interception of wire and oral communications

Be it enacted by the Senate and House of Representative of the United States of America in Congress assembled, That section 2511 of title 18 of the United States Code is amended by adding at the end thereof the following:

"(4) Notwithstanding any other law or provision of law, whoever, acting under color of law, intercepts or discloses any wire or oral communication,

with respect to which a judge or justice of the United States or a Senator or Member of Congress is a party, without the written authorization of the President (specifically authorizing the particular interception or disclosure) shall be fined not more than $20,000 or imprisoned not more than ten years, or both."

[H. R. 7773, 93d Cong., 1st sess.]

A BILL To amend title XII of the Organized Crime Control Act of 1970, and for other purposes

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That title XII of the Organized Crime Control Act of 1970 (84 Stat. 922, 960) is amended as follows:

(a) The heading of the title is amended to read:

"TITLE XII—NATIONAL COMMISSION ON INDIVIDUAL RIGHTS AND PERSONAL SECURITY"

(b) Section 1201 is amended by adding "and Personal Security" after the word "Rights".

(c) Section 1204 is amended to read as follows:

"SEC. 1204. It shall be the duty of the Commission to conduct a comprehensive study and review of Federal court decisions, laws, and practices relating (1) to special grand juries authorized under chapter 216 of title 18, United States Code, dangerous special offender sentencing under section 3575 of title 18, United States Code, bail reform and preventive detention, no-knock search warrants, the accumulation of data on individuals by Federal agencies as authorized by law or acquired by executive action, and (2) the conduct of stop and frisk arrests, searches and seizures, interrogations, appellate review by the prosecution, lack of mutual pretrial criminal discovery, self-incrimination and prosecutor comment on failure to testify, the conduct of lineups, disclosure of informants' identities, fingerprinting and photography, and trial delay, finality and collateral review of Federal and State criminal proceedings. The Commission may also consider other Federal court decisions, laws, and practices which in its opinion may infringe upon the individual rights of the people of the United States to liberty or to personal security. The Commission shall determine which legal rules, laws, and practices are needed, which are effective, and whether they infringe upon the individual rights of the people of the United States to liberty or to personal security."

(d) Section 1207 is amended to read as follows:

"SEC. 1207. (a) The Commission or any duly authorized subcommittee or member thereof may, for the purpose of carrying out the provisions of this title, hold such hearings, sit and act at such times and places, administer such oaths, and require by subpena or otherwise the attendance and testimony of such witnesses and the production of such books, records, correspondence, memorandums, papers, and documents as the Commission or such subcommittee or member may deem advisable. Any member of the Commission may administer oaths or affirmations to witnesses appearing before the Commission or before such subcommittee or member. Subpenas may be issued under the signature of the Chairman or any duly designated member of the Commission, and may be served by any person designated by the Chairman or such member.

"(b) In the case of contumacy or refusal to obey a subpena issued under subsection (a) by any person who resides, is found, or transacts business within the jurisdiction of any district court of the United State, the district court, at the request of the Chairman of the Commission, shall have jurisdiction to issue to such person an order requiring such person to appear before the Commission or a subcommittee or member thereof, there to produce evidence if so ordered, or there to give testimony touching the matter under inquiry. Any failure of any such person to obey any such order of the court may be punished by the court as a contempt thereof.

"(c) The Commission is an 'agency of the United States' under subsection (1) of section 6001 of title 18, United States Code, for the purpose of granting immunity to witnesses.

"(d) Each department, agency, and instrumentality of the executive branch of the Government, including independent agencies, is authorized and directed

to furnish to the Commission, upon request made by the Chairman, on a reimbursable basis or otherwise, such statistical data, reports, and other information as the Commission deems necessary to carry out its functions under this title. The Chairman is further authorized to call upon the departments, agencies, and other offices of the several States to furnish, on a reimbursable basis or otherwise, such statistical data, reports, and other information as the Commission deems necessary to carry out its functions under this title."

(e) Section 1208 is amended to read as follows:

"SEC. 1208. The Commission may make interim reports and recommendations as it deems advisable, and it shall make a final report of its findings and recommendations to the President of the United States and to the Congress at the end of three years following the date of enactment of this amendment to this section. Sixty days after the submission of the final report, the Commission shall cease to exist."

[H. R. 9667, 93d Cong., 1st sess.]

A BILL To amend title 18 of the United States Code to require the consent of all persons whose communications are intercepted under certain provisions relating to certain types of eavesdropping

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That section 2511(2) of title 18 of the United States Code is amended by striking out paragraphs (c) and (d), and inserting in lieu thereof the following:

"(c) It shall not be unlawful under this chapter for a person to electronically record or otherwise intercept a wire or oral communication where all parties to the communication have given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State or for the purpose of committing any other injurious act."

[H. R. 9698, 93d Cong., 1st sess.]

A BILL To amend title 18 of the United States Code to prohibit the interception of certain communications unless all parties to the intercepted communication consent

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That section 2511 of title 18 of the United States Code is amended by—

(1) striking out, in subsection (2)(c), "or one of the parties to such interception" and inserting in lieu thereof ", but only if all of the parties to the communication have given prior consent to such interception."; and

(2) striking out, in subsection 2(d), "or where one of the parties to the communication has given prior consent to such interception" and inserting in lieu thereof ", but only if all of the parties to the communication have given prior consent to such interception,".

[H. R. 9781, 93d Cong., 1st sess.]

A BILL To amend certain sections (authorizing wiretapping and electronic surveillance) of title 18 of the United States Code

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That the Congress finds and declares that—

(1) Widespread wiretapping and electronic surveillance, both by private persons and Government agents, both under color of law, and without pretense of legal excuse or justification, has seriously undermined personal security and often violated fundamental constitutional rights, including the rights to free speech, press, and association, the rights to due process and equal protection, and the right to privacy.

(2) Complexities and defects in current Federal law have aided those who engage in wiretapping and electronic surveillance, and current Federal law has not provided adequate safeguards against corrupt abuses of communications technology.

(3) No person, in any branch of the Federal Government, in however high an office, or in any other governmental or private position should be authorized either explicitly or implicitly to violate the constitutional rights of persons by eavesdropping on private conversations through wiretapping and electronic surveillance.

(4) The end of prosecuting those who violate the law does not justify wrongdoing on the part of the Government.

(5) The peculiar susceptibility of wiretapping and electronic surveillance to misuse in the furtherance of partisan political goals renders wiretapping and electronic surveillance a particularly dangerous temptation to Government officials, and the chance of its misuse outweighs any potential benefits which might otherwise be found in it.

SEC. 2. Title 18 of the United States Code is amended—

(1) by striking out in section 2511(1) "Except as otherwise specifically provided in this chapter any person who—" and inserting in lieu thereof "Whoever—";

(2) by inserting immediately after subparagraph (d) of section 2511(1), but before "shall be fined" the following new subparagraph:

"(e) willfully intercepts or records any wire or oral communication without the consent of all the parties to such communication";

(3) by striking out "or" at the end of section 2511 (1) (c) and by inserting "or" at the end of section 2511(1)(d);

(4) by striking out sections 2511(2)(a)(ii), (b), (c), and (d);

(5) by striking out section 2511(3);

(6) by striking out section 2512(1) "Except as otherwise provided in this chapter, any person who willfully—" and inserting in lieu thereof "Whoever—";

(7) by striking out section 2512(2); and

(8) by striking out sections 2516, 2517, 2518, 2519, 2510(9).

[H. R. 9815, 93d Cong., 1st sess.]

A BILL To enforce the first amendment and fourth amendment to the Constitution, and the constitutional right of privacy by prohibiting any civil or military officer of the United States or the militia of any State from using the Armed Forces of the United States or the militia of any State to exercise surveillance of civilians or to execute the civil laws, and for other purposes

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. This Act may be cited as the "Freedom from Surveillance Act of 1973".

SEC. 2. (a) Chapter 67 of title 18, United States Code, is amended by adding at the end thereof the following new sections:

"§ 1386. Use of the Armed Forces of the United States for surveillance prohibited

"(a) Except as provided in subsection (b) of this section, whoever being a civil officer of the United States or an officer of the Armed Forces of the United States employs any part of the Armed Forces of the United States or the militia of any State to conduct investigations into, maintain surveillance over, or record or maintain information regarding, the beliefs, associations, or political activities of any person not a member of the Armed Forces of the United States, or any civilian organization, shall be fined not more than $10,000, or imprisoned not more than two years, or both.

"(b) The provisions of this section shall not apply to the use of the Armed Forces of the United States or the militia of any State:

"(1) to do anything necessary or appropriate to enable such forces or militia to accomplish their mission after they have been actually and publicly assigned by the President to the task of repelling invasion or suppressing rebellion, insurrection, or domestic violence, pursuant to the Constitution or section 331, section 332, or section 333 of title 10 of the United States Code; or

"(2) to investigate criminal conduct committed on a miliary installation or involving the destruction, damage, theft, unlawful seizure, or trespass of the property of the United States; or

"(3) to determine the suitability for employment or for retention in employment of any individual actually seeking employment or employed by the Armed Forces of the United States or by the militia of any State, or by a defense facility; or

"(4) whenever the militia of any State is under the command or control of the chief executive of that State or any other appropriate authorities of that State.

"(c) As used in this section, the term—

"(1) 'Armed Forces of the United States' means the Army, Navy, Air Force, Marine Corps, and Coast Guard;

"(2) 'militia' has the same meaning as that set forth in section 311 of title 10, United States Code;

"(3) 'civil officer of the United States' means any civilian employee of the United States;

"(4) 'surveillance' means any monitoring conducted by means which include but are not limited to wiretapping, electronic eavesdropping, overt and covert infiltration, overt and covert observation, and civilian informants;

"(5) 'defense facility' has the same meaning as that set forth in section 782(7) of title 50, United States Code.".

(b) The analysis of chapter 67 of such title is further amended by adding at the end thereof the following new item:

"1386. Use of Armed Forces of the United States for surveillance prohibited.".

SEC. 3. (a) Title 28, United States Code, is amended by adding after chapter 171 the following new chapter:

"Chapter 172.—ILLEGAL SURVEILLANCE

"Sec.
"2691. Civil actions, generally; illegal surveillance.
"2692. Special class actions; illegal surveillance.
"2693. Venue.

"§ 2691. Civil actions, generally; illegal surveillance

"(a) Whenever any person is aggrieved as a result of any act which is prohibited by section 1386 of title 18, United States Code, such a person may bring a civil action for damages irrespective of the actuality or amount of pecuniary injury suffered.

"(b) Whenever any person is threatened with injury as a result of any act which is prohibited by section 1386 of such title, such a person may bring a civil action for such equitable relief as the court determines may be appropriate irrespective of the actuality or amount of pecuniary injury threatened.

"§ 2692. Class action; illegal surveillance

"Whenever any person has reason to believe that a violation of section 1386 of title 18, United States Code, has occurred or is about to occur, such person may bring a civil action on behalf of himself and others similarly situated against any civil office of the United States or any military officer of the Armed Forces of the United States to enjoin the planning or implementation of any activity in violation of that section.

"§ 2693. Venue

"A person may bring a civil action under this chapter in any district court of the United States for the district in which the violation occurs, or in any district court of the United States for the district in which the violation occurs, or in any district court of the United States in which such person resides or conducts business, or has his principal place of business, or in the District Court of the United States for the District of Columbia.".

(b) The analysis of part VI of such title 28 is amended by adding immediately after item 171 the following new item:

"172. Illegal surveillance ---------- 2691".

(c) Section 1343 of title 28, United States Code, is amended by redesignating paragraph (4) as paragraph (5) and by inserting immediately after paragraph (3) the following new paragraph:

"(4) To recover damages or to secure equitable or other relief under chapter 172 of this title;".

SEC. 4. The civil actions provided by the amendments to title 28, United States Code, made by this Act shall apply only with respect to violations of section 1386 of title 18, United States Code, as added by this Act, arising on or after the date of enactment of this Act.

SEC. 5. (a) Section 1385 of title 18, United States Code, is amended by striking out "the Army or the Air Force" and inserting in lieu thereof the following: "the Armed Forces of the United States".

(b) (1) The section heading of section 1385 of such title is amended to read as follows:

(2) Item 1385 of the analysis of chapter 67 is amended to read as follows:

"1385. Use of Armed Forces of the United States as posse comitatus.".

[H. R. 9973, 93d Cong., 1st sess.]

A BILL To amend title 18 of the United States Code to require the consent of all persons whose communications are intercepted under certain provisions relating to certain types of eavesdropping

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That section 2511(2) of title 18 of the United States Code is amended by striking out paragraphs (c) and (d), and inserting in lieu thereof the following:

"(c) It shall not be unlawful under this chapter for a person to electronically record or otherwise intercept a wire or oral communication where all parties to the communication have given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violating of the Constitution or laws of the United States or of any State or for the purpose of commiting any other injurious act.".

[H. R. 9949, 93d Cong., 1st sess.]

A BILL To clarify the meaning of certain provisions of the Criminal Code relating to unlawful interception of communications and other provisions of law

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That section 2511 of title 18, United States Code, is amended by adding the following new sentence to the end of paragraph (3) thereof: "Nothing contained in this paragraph shall be deemed to authorize the President, or anyone acting or purporting to act on his behalf, to engage in burglary or any other illegal act that is not prohibited by this chapter.".

SEC. 2. Nothing contained in any provision of law heretofore or hereafter enacted by the Congress shall be deemed to authorize the President, or anyone acting or purporting to act on his behalf, to engage in burglary or any other illegal act that a statute of the Congress does not expressly and explicitly authorize the President or his delegate to engage in.

[H. R. 10008, 93d Cong., 1st sess.]

A BILL To amend title 18 of the United States Code to require the consent of all persons whose communications are intercepted under certain provisions relating to certain types of eavesdropping

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That section 2511(2) of title 18 of the United States Code is amended by striking out paragraphs (c) and (d), and inserting in lieu thereof the following:

"(c) It shall not be unlawful under this chapter for a person to electronically record or otherwise intercept a wire or oral communication where all parties to the communication have given prior consent to such interception unless such communication is intercepted for the purpose of commiting any criminal or tortious act in violation of the Constitution or laws of the United States or of any State or for the purpose of committing any other injurious act."

[H. R. 10331, 93d Cong., 1st sess.]

A BILL To amend title 18 of the United States Code to require the consent of all persons whose communications are intercepted under certain provisions relating to certain types of eavesdropping

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That section 2511(2) of title 18 of the United States code is amended by striking out paragraphs (c) and (d), and inserting in lieu thereof the following:

"(c) It shall not be unlawful under this chapter for a person to electronically record or otherwise intercept a wire or oral communication where all parties to the communication have given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State or for the purpose of committing any other injurious act.".

[H. R. 11629, 93d Cong., 1st sess.]

A BILL To enforce the first amendment and fourth amendment to the Constitution and the constitutional right of privacy by prohibiting any civil or military officer of the United States or the militia of any State from using the Armed Forces of the United States or the militia of any State to exercise surveillance of civilians or to execute the civil laws, and for other purposes

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. This Act may be cited as the "Freedom From Surveillance Act of 1973".

SEC. 2. (a) Chapter 67 of title 18, United States Code, is amended by adding at the end thereof the following new sections:

"§ 1386. Use of the Armed Forces of the United States for surveillance prohibited

"(a) Except as provided in subsection (b) of this section, whoever being a civil officer of the United States or an officer of the Armed Forces of the United States employs any part of the Armed Forces of the United States or the militia of any State to conduct investigations into, maintain surveillance over, or record or maintain information regaarding, the beliefs, associations, or political activities of any person not a member of the Armed Forces of the United States, or of any civilian organization, shall be fined not more than $10,000, or imprisoned not more than two years, or both.

"(b) The provisions of this section shall not apply to the use of the Armed Forces of the United States or the militia of any State—

"(1) when they have been actually and publicly assigned by the President to the task of repelling invasion or suppressing rebellion, insurrection, or domestic violence pursuant to the Constitution or section 331, section 332, or section 333 of title 10 of the United States Code; or

"(2) to ivestigate criminal conduct committed on a military installation or involving the destruction, damage, theft, unlawful seizure, or trespass of the property of the United States; or

"(3) to determine the suitability for employment or for retention in employment of any individual actually seeking employment or employed by the Armed Forces of the United States or by the militia of any State, or by a defense facility; or

"(4) whenever the militia of any State is under the command or control of the chief executive of that State or any other appropriate authorities of that State.

"(c) As used in this section, the term—

"(1) 'Armed Forces of the United States' means the Army, Navy, Air Force, Marine Corps, and Coast Guard;

"(2) 'militia' has the same meaning as that set forth in section 311 of title 10, United States Code;

"(3) 'civil officer of the United States' means any civilian employee of the United States;

"(4) 'surveillance' means any monitoring conducted by means which include but are not limited to wiretapping, electronic eavesdropping, overt

and covert infiltration, overt and covert observation, and civilian informants;

"(5) 'defense facility' has the same meaning as that set forth in section 782(7) of title 50, United States Code.".

(b) The analysis of chapter 67 of such title is further amended by adding at the end thereof the following new item:

"1386. Use of Armed Forces of the United States for surveillance prohibited.".

SEC. 3. (a) Title 28, United States Code, is amended by adding after chapter 171 the following new chapter:

"Chapter 172.—ILLEGAL SURVEILLANCE

"Sec.
"2691. Civil actions, generally; illegal surveillance.
"2692. Class action; illegal surveillance.
"2693. Venue.

"§ 2691. Civil actions, generally; illegal surveillance

"(a) Whenever any person is aggrieved as a result of any act which is prohibited by section 1386 of title 18, United States Code, such a person may bring a civil action for damages irrespective of the actuality or amount of pecuniary injury suffered.

"(b) Whenever any person is threatened with injury as a result of any act which is prohibited by section 1386 of such title, such a person may bring a civil action for such equitable relief as the court determines may be appropriate irrespective of the actuality or amount of pecuinary injury threatened.

"2692. Class action; illegal surveillance

"Whenever any person has reason to believe that a violation of section 1386 of title 18, United States Code, has occurred or is about to occur, such person may bring a civil action on behalf of himself and others similarly situated against any civil officer of the United States or any military officer of the Armed Forces of the United States to enjoin the planning or implementation of any activity in violation of that section.

"§ 2693. Venue

"A person may bring a civil action under this chapter in any district court of the United States or the district in which the violation occurs, or in any district court of the United States in which such person resides or conducts business, or has his principal place of business, or in the District Court of the United States for the District of Columbia.".

(b) The analysis of part VI of such title 28 is amended by adding immediately after item 171 the following new item:

"172. Illegal surveillance ---------- 2691".

(c) Section 1343 of title 28, United States Code, is amended by redesignating paragraph (4) as paragraph (5) and by inserting immediately after paragraph (3) the following new paragraph:

"(4) To recover damages or to secure equitable or other relief under chapter 172 of this title;".

SEC. 4. The civil actions provided by the amendments to title 28, United States Code, made by this Act shall apply only with respect to violations of section 1386 of title 18, United States Code, as added by this Act, arising on or after the date of enactment of this Act.

SEC. 5 (a) Section 1385 of title 18, United States Code, is amended by striking out "the Army or the Air Force" and inserting in lieu thereof the following: "the Armed Forces of the United States."

(b)(1) The section heading of section 1385 of such title is amended to read as follows:

"§ 1385. Use of Armed Forces of the United States as posse comitatus".

(2) Item 1385 of the analysis of chapter 67 is amended to read as follows:

"1385. Use of Armed Forces of the United States as posse comitatus.".

[H. R. 11838, 93d Cong., 1st sess.]

A BILL To amend sections 2516 (1) and (2) of title 18 of the United States Code to assure that all wiretaps and other interceptions of communications which are authorized under that section have prior court approval

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That section 2516(1) and (2) of title 19 of the United States Code are amended in both instances—

(1) by striking out "an order authorizing or approving" and inserting in lieu thereof "an order giving prior authorization to"; and

(2) by striking out "when such interception may provide or has provided" and inserting in lieu thereof "when such interception may provide".

[H. R. 13825, 93d Cong., 2d sess.]

A BILL To establish administrative and governmental practices and procedures for certain kinds of surveillance activities engaged in by the administrative agencies and departments of the Government when executing their investigative, law enforcement, and other functions, and for other purposes

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Surveillance Practices and Procedures Act of 1974".

SEC. 2. The Congress hereby finds and declares that—

(a) Recent events have uncovered abuses by certain administrative agencies, departments, and other units of the Government, when engaging in certain surveillance practices, including the use of wiretaps, for investigative, law enforcement, and other purposes.

(b) Those abuses referred to in subsection (a) have undermined and/or threatened to undermine the individual's right to privacy and other constitutional rights and liberties.

(c) The public has expressed deep concern that abusive practices and procedures by governmental agencies, departments, and/or other units of the Government when engaging in surveillance activities for investigative, law enforcement, and other purposes, may continue to undermine and/or threaten to undermine the individual's right to privacy and other constitutional rights and liberties.

(d) There is a need for the administrative agencies and departments of the Government to engage in certain surveillance practices and procedures in order to properly and satisfactorily execute their lawful investigative, law enforcement, and other functions.

(e) Congress should establish practices and procedures to be followed by the administrative agencies, departments, and other units of the Government when engaging in certain surveillance activities so as to reconcile the interest of the Government in properly and satisfactorily executing its investigative law enforcement, and other functions with the interest of the Congress and the public in protecting the integrity of the individual's right to privacy and other constitutional rights and liberties.

(f) The need for the practices and procedures described in subsection (e) is particularly acute in cases involving the use of wiretaps and other electronic surveillance by the administrative agencies, departments, and other units of the Government when executing their investigative, law enforcement, and other functions.

SEC. 3. (a) Section 2510(10) of title 18, United States Code, is amended by deleting after "Code;" the following: "and".

(b) Section 2510(11) of title 18, United States Code, is amended by adding after "directed" the following: "; and".

(c) Section 2510 of title 18, United States Code, is amended by adding immediately after subsection (11) the following:

"(12) 'foreign agent' means any person who is not an American citizen or in the process of becoming an American citizen and whose first allegiance is to a foreign power and whose activities are intended to serve the interest of that foreign power and to undermine the security of the United States.".

SEC. 4. (a) The first sentence of section 2511(3) of title 18, United States Code, is amended by inserting immediately after "measures" the following: "against foreign powers and foreign agents, pursuant to the procedures delineated in section 2518A,".

(b) Section 2511(3) of title 18, United States Code, is amended by deleting the second sentence.

(c) Section 2511(3) of title 18, United States Code, is amended by striking out the third sentence and adding in lieu thereof the following: "Notwithstanding any other provision of this chapter, neither the contents, nor the evidence derived therefrom, of any wire or oral communication intercepted through application of this subsection shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court, except in civil proceedings against foreign agents.".

SEC. 4A. Section 2516 of title 18, United States Code, is amended by deleting subsection (a); subsection letters "(b)", "(c)", "(d)", "(e)", "(f)", and "(g)" of section 2516 shall be deleted and the respective subsections shall be identified as "(a)", "(b)", "(c)", "(d)", "(e)", and "(f)".

SEC. 5. (a) Chapter 119 of title 18, United States Code, is amended by adding immediately after section 2516 thereof the following new section:

"§ 2516A. Authorization for interception of wire or oral communication in national security cases

"The Attorney General, or any Assistant Attorney General specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518A of this chapter, an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or any Federal administrative agency, department, or other unit having lawful responsibility for the investigations of the offense as to which application is made, when—

"(1) there is probable cause to believe that the individual(s) whose oral or wire communications are to be intercepted has committed or is about to commit an offense punishable by death or by imprisonment for more than one year under—

"(a) sections 2274 through 2277 of title 42 of the United States Code (relating to enforcement of the Atomic Energy Act of 1954), or

"(b) one of the following chapters of this title: chapter 37 (relating to espionage), chapter 105 (relating to sabotage), and chapter 115 (relating to treason); and

"(2) such interception will probably provide or has provided evidence concerning the commission of that offense.".

(b) Chapter 119 of title 18, United States Code, is amended by adding immediately after section 2518 thereof the following new section:

"§ 2518A. Procedure for interception of wire or oral communication relating to national security

"(1) Each application for an order authorizing or approving the interception of a wire or oral communication under section 2511(3) or section 2516A of this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction, or, in cases involving section 2511(3), a judge on the Federal District Court for the District of Columbia, and shall state the applicant's authority to make such application. Each application shall include the following information:

"(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

"(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) a description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (ii) a description of the communications, with as much particularity as is possible and practical, sought to be intercepted, (iii) the identity of the person, if known, whose communications are to be intercepted, and (iv) in cases involving application of section 2516A, details as to the particular offense that has been, is being, or is about to be committed;

"(c) a detailed statement as to whether or not other investigative procedures have been tried and failed or why they appear to be unlikely to succeed if tried or to be too dangerous;

"(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described communications have been first obtained, a description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

"(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire or oral communications involving any of the same persons, facilities, or places specified in the application, and the action taken by the judge on each such application; and

"(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

"(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application. But in no event may authorization or approval of any wire or oral communication be granted unless the applicant furnishes evidence, independent of his and others conclusory opinion, that such interception shall serve one of the purposes set forth in section 2511(3) or section 2516A above.

"(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire or oral communications within the territorial jurisdiction of the court in which the judge is sitting, or, in cases involving section 2511(3) when application has been made to a judge on the Federal District Court for the District of Columbia, anywhere within the territorial jurisdiction of the United States, if the judge determines on the basis of the facts submitted by the applicant that—

"(a) there is probable cause for belief that the interception is necessary in order to gain information serving one of the purposes set forth in section 2511(3) or section 2516A;

"(b) there is probable cause for belief that particular communications concerning one of the purposes set forth in section 2511(3) or section 2516A will be obtained through such interceptions;

"(c) normal investigative procedures have been tried and have failed to appear to be unlikely to succeed if tried or to be too dangerous; and

"(d) there is probable cause for belief that the facilities from which, or the place where, the wire or oral communications are to be intercepted are being used or are about to be used by the subject whose wire or oral communications are to be intercepted.

"(4) Each order authorizing or approving the interception of any wire or oral communication shall specify—

"(a) the identity of the person, if known, whose communications are to be intercepted;

"(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

"(c) a description of the type of the communication sought to be intercepted;

"(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

"(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

"(5) No order entered under this section may authorize or approve the interception of any wire or oral communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than fifteen days. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of

this section and the court making anew the findings required by subsection (3) of this section. In making this new finding under subsection (3), the judge shall, in cases involving section 2516A, require the applicant to furnish additional information and evidence independent of that relied upon in granting the intial order and which, standing alone, would satisfy the requirements of subsection (3). The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than ten days. Every order and extension thereof shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in fifteen days.

"(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order shall require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such report shall be made at such intervals as the judge may require.

"(7) The contents of any wire or oral communication intercepted by any means authorized by section 2511(3) or section 2516A shall be subject to the requirements of section 2518(8)(a). Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs.

"(8) Notwithstanding any other provision of this chapter, any individual, other than a foreign agent, whose wire or oral communications have been intercepted through application of section 2511(3) or section 2516A shall, not less than thirty days after the expiration of a judicial order authorizing such interception, be furnished a copy of the court order(s), and accompanying application(s), under which such interception was authorized or approved, and a complete and accurate transcript or other record of the intercepted communication, such transcript or record to also include the date(s) and time(s) at which such interception occurred: *Provided*, That, upon application of the Attorney General, or any Assistant Attorney General specially designated by the Attorney General, the judge who authorized or approved the interception may postpone the disclosure of such interception if he is satisfied that the individual whose communications have been intercepted is engaged in a continuing criminal enterprise or conspiracy and disclosure of the interception will endanger vital national security interests, such postponement to be as long as the judge deems necessary: *And provided further*, That any interception, disclosed pursuant to this subsection and which involves application of section 2511(3), need not disclose the foreign power or agent whose wire or oral communications were intended to be intercepted, nor those facilities at which the interception was intended to or did take place.

"(9)(a) Notwithstanding any other provision of this chapter, any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any intercepted wire or oral communication, or evidence derived therefrom, on the grounds that—

"(i) the communication was unlawfully intercepted;

"(ii) the order of authorization or approval under which it was intercepted is insufficient on its face;

"(iii) the interception was not made in conformity with the order of authorization or approval; or

"(iv) subsection 2511(3) requires such suppression.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter.

"(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is

not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.".

SEC. 6. (a) The analysis of chapter 119 of title, 18 United States Code, is amended by inserting immediately after the item

"2516. Authorization for interception of wire or oral communications."

the following new item:

"2516A. Authorization for interception of wire or oral communications in national security cases.".

(b) Such analysis is further amended by inserting immediately after the item

"2518. Procedure for interception of wire or oral communications."

the following new item:

"2518A. Procedure for interception of wire or oral communications relating to national security.".

SEC. 7. Section 2519(1) is amended by inserting immediately after "2518," the following: "or section 2518A.".

Mr. KASTENMEIER. Our first witness this morning has long expressed his concern on this subject and is a chief sponsor of Senate legislation to require court approval for all wiretapping and electronic surveillance, including national security wiretapping. I am pleased to welcome a fellow member of the Wisconsin Delegation and my good friend Senator Gaylord Nelson.

TESTIMONY OF HON. GAYLORD NELSON, A U.S. SENATOR FROM THE STATE OF WISCONSIN

Senator NELSON. Mr. Chairman, and members of the committee, there is a Democratic Conference at the Senate side that I need to get to, so if it is all right with the chairman, I would ask that my full statement be printed in the record as so read, and then I would like to submit for the record some materials in support of the statement.

The first item is a statement which details the history of abuses in the use of warrantless wiretaps for so-called "national security cases," and the second item is a section-by-section analysis of the Surveillance Practices and Procedures Act to prohibit warrantless wiretaps. It shows quite clearly that every section of the bill is fully supported by historical and legal precedents. Finally, I would like to submit some newspaper columns and editorials which discuss the importance of a bill to prohibit warrantless wiretaps.

Mr. KASTENMEIER. Without objection, your 11-page statement will be received and made a part of the record and the additions you have described will also be received.

[The documents referred to appear at p. 29.]

Senator NELSON. Mr. Chairman it seems to me the time is long past due for congressional action to check the dangerous abuses of government wiretapping and other surveillance activities.

The need for action, and therefore the importance of this subcommittee's inquiry, are quite clear. Uncontrolled government wiretaps and other surveillance activities constitute an intolerable threat to fundamental constitutional rights and liberties. Individual free-

dom—the cornerstone of our democratic system—is but an illusion in a society where the government can invade an individual's privacy at will.

Until recently, most of the public did not appreciate the inherent dangers of government snooping. Now the public understands that government snooping poses a real threat to everyone, regardless of his or her station in life. Now 77 percent of the public favors legislation to curb the abuses of government wiretapping and spying.

Hearings by the Senate Watergate Committee and other congressional bodies as well as reports by various periodicals exposed in great detail how the government could and did invade the privacy of law-abiding individuals. Reference to just a few recent examples is sufficient to illustrate the magnitude of dangers of government snooping:

Now, Mr. Chairman, I list a series of examples, all of which have been either publicized in the papers or presented to committees on either the House or Senate side, so I will not read them into the record.

For many years constitutional authorities and other citizens have repeatedly expressed alarm over the rapidly expanding practice of governmental invasions of privacy by wiretapping, data collection, and other forms of surveillance. In 1967 I made a speech on the floor of the Senate on this issue and in 1971 introduced legislation to establish a joint congressional committee to control Government snooping.

Mr. Chairman and members of the committee, this specific proposal that is before the committee today refers to warrantless wiretaps. That is just one step that needs to be taken by the Congress to protect the constitutional rights of citizens. There is a further step which the Congress must also take up at some subsequent date, and that is a step that will insure that the Constitution and the law are complied with. I have introduced legislation on our side on this issue. This legislation proposes creation of a joint committee of the House and Senate, a bipartisan committee with equal representation by each party. Each year every agency of the Government which has or asserts any power or authority to spy—such as the military intelligence, the FBI, and others—must come before that committee and present to that committee, either publicly or in executive session, a record of all of the wiretaps and surveillance of any kind that was performed by that agency, the legal justification for it, and the purpose of it. All of this would be presented under oath with the penalty of perjury, of course. The purpose of this would be to enable the people's representatives to guarantee that the Constitution and the statutes are complied with and furthermore, Mr. Chairman, for the Congress to be informed as to what kind of activities are engaged in by these agencies so that we may decide if further legislation is necessary.

I think that piece of legislation is critical to assuring compliance with any other legislation that we pass and to assure compliance with the fourth amendment of the Constitution.

The bill entitled "Surveillance Practices and Procedures Act of 1973" is before the subcommittee and has been introduced on both sides by myself in the Senate and by the chairman of this subcommittee in the House of Representatives.

The bill is a direct response to wiretap abuses in so-called national security cases. Last May it was revealed that in 1969 the White House bypassed established procedures and authorized wiretaps on the telephones of 17 Government officials and newspapermen. The purported basis of these taps was a concern that sensitive information was being leaked to reporters by Government officials. The Government, however, did not obtain a judicial warrant before installing the taps. The Government alone decided whom it would tap and for how long.

Subsequent investigation showed that some of the Government officials tapped did not have access to sensitive information. It was also learned that two of the taps were maintained after the individuals involved had left Government service and joined the Presidential campaign staff of Senator Muskie. In none of the cases was the individual suspected of having violated the law.

These are not isolated incidents. Warrantless taps based on so-called national security reasons were placed on the telephones of newspaper columnist Joseph Kraft in 1969 and in 1971 on friends of a Navy yeoman suspected of passing sensitive information to the Joint Chiefs of Staff. Again, none of these individuals was even suspected of having violated the law.

The use of so-called national security taps, however, has not been confined to the present administration. Democratic and Republican administrations since the 1930's have used such taps to spy on law-abiding individuals. Various government reports indicate that since that time thousands of individuals have had their telephone conversations intercepted for so-called national security reasons.

From the very beginning, those sensitive to civil liberties recognized the dangers of warrantless wiretaps. Such taps enable the Government to exercise unchecked and unreviewed power over the individual. There is no opportunity for a court, the Congress, or the public to demonstrate that the taps are unreasonable. For this reason, Supreme Court Justice Oliver Wendell Holmes called them dirty business. In my view, such taps are also clearly unconstitutional.

To understand the basis of this opinion it is necessary to examine the language and judicial interpretation of the fourth amendment. That amendment states quite simply that:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

That language is clear and unequivocal. It allows for no exception.

One need not be an historian or a lawyer to understand the essential purpose of this amendment. It is intended to protect the individual's privacy from unreasonable invasions by the Government.

To afford this protection, the amendment contemplates that a neutral court—not the Government—will determine whether any search and seizure planned by the Government is reasonable. Otherwise the Government would be both advocate and judge of its own case.

The fourth amendment thus limits the power of the Government. Like the other amendments in the Bill of Rights, it reflects the framers' intention that individual liberty, rather than unrestrained governmental power, be the hallmark of our political system. In his dissent in the 1928 *Olmstead* case Supreme Court Justice Louis Brandeis articulated the importance of the fourth amendment in our scheme of government:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions, and their sensations. They 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 unjustified intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the fourth amendment.

The fourth amendment's protections apply to all Government searches and seizures. No exception is made for national security cases or any other kind of circumstance.

When the Constitution was drafted in 1787, our country was only 11 years old. The new American citizens had recently concluded a long war with England to preserve their country's independence. That independence was not entirely secure. The threat of foreign attack and subversion remained ever present. Despite the existence of this threat, the Founding Fathers adopted the fourth amendment and made no exception to its application.

In the 1967 *Berger* and *Katz* cases, the Supreme Court held that the fourth amendment applies to wiretapping for criminal purposes. In effect, these decisions required the government to obtain an approving judicial warrant before it could install a wiretap in a criminal investigation.

In the 1972 *Keith* case the Court, by an 8–0 vote, decided further that the Government could not wiretap individuals without a judicial warrant even when the individual's activities threatened the Nation's "domestic security." Again, the Court made clear that wiretaps must adhere to the safeguards delineated by the fourth amendment:

> "Though physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed, the broader spirit now shields private speech from unreasonable surveillance.

The Supreme Court has not yet decided whether the fourth amendment's protections apply to cases involving the activities of foreign powers and their agents. In the *Keith* case, the court stated explicitly that it did not consider those situations where American citizens have a "significant connection" with foreign powers and their agents.

Because the Court has not ruled on these "national security" taps, the present administration maintains that it may install warrantless wiretaps in certain situations. In a September 1973 letter to Senator William Fulbright, chairman of the Senate Foreign Relations Committee, then Attorney General Elliot Richardson stated that the administration would continue to install warrantless wiretaps against American citizens and domestic organizations if the administration believes their activities affect "national security" matters—although "national security" is never defined.

Mr. Richardson's comments apparently still reflect administration policy. Last January the Justice Department reported that it had authorized three warrantless wiretaps for national security reasons—an average week's quota according to the Department. The Department did not explain to any neutral party such as the Court the justification for the taps or identify the subjects of the taps.

The continued use of warrantless wiretaps for so-called national security reasons underscores the need for congressional action. People in our country should not be afraid to speak to one another on the telephone, never knowing whether the Government is listening or how the Government might use any information obtained. Every citizen should be assured that the privacy of his or her telephone conversations will not be invaded unless a neutral court first determines that the invasion is justified pursuant to the Constitution.

The Surveillance Practices and Procedures Act is designed to provide that assurance. The bill includes three principal provisions.

First, before it could wiretap American citizens for national security reasons, the Government would have to obtain a judicial warrant based on probable cause that a specific crime has been or is about to be committed. This provision would thus protect an individual's privacy against unjustified national security wiretaps.

Second, before the Government could wiretap a foreign power or its agents, it would have to obtain a judicial warrant based on the belief that the tap is necessary to protect national security interests. The warrant standards for foreign powers and their agents would thus be less rigorous than those required for American citizens. This warrant requirement will in no way undermine the government's ability to protect against foreign attack or subversion; the government will be able to wiretap foreign powers and their agents any time there is a need for such surveillance and the need is presented to the court.

The justification for this second warrant procedure is plain. The Government's desire to wiretap should be reviewed by a court in all instances.

Third, every American citizen wiretapped would be informed of the surveillance with 30 days after the last authorized interception. This provision would assure every wiretapped American citizen the opportunity to protect against violations of his or her constitutional rights. The disclosure of the wiretap could be indefinitely postponed, however, if the Government satisfies the court that the person wiretapped is engaged in a continuing criminal enterprise

that would involve, for example, organized crime activities, or that disclosure would endanger national security interests.

The need for legislation such as this should be beyond dispute. Warrantless wiretaps—whether for "national security" reasons or other purposes—pose a grave danger to individual rights of speech and privacy. Such taps invest the Government with an absolute power over the individual. They enable the Government to pry into an individual's private affairs without justification. They foster the reality of an Orwellian state in which the government becomes a monster to be feared rather than a servant to be trusted.

That is not the kind of government envisioned by our Founding Fathers. The underlying and fundamental premise of our Constitution is that all Government power is limited by checks and balances. This is no less true of the Government's power to protect "national security." That power is not so absolute that it can excuse infringements of the right to privacy and other constitutional liberties. It would indeed be ironic if the government could invoke "national security" to violate those individual freedoms which the government is obligated to defend.

Mr. Chairman, I think I have covered everything that needs to be covered on my testimony.

Mr. KASTENMEIER. Thank you, Senator Nelson, for your very compelling testimony. I have just a couple of questions.

While it may be said that one could determine what is crime in the Federal system and what is not a crime, are you satisfied that there is any definition as to what constitutes "national security" or "national security interest" for these purposes?

Senator NELSON. There is none. In the past, national security has been what the users of the wiretap considered national security to be. So during the Vietnam war and during the demonstrations, the National Council of Churches was invaded by military intelligence people, and all kinds of people were spied on if they attended a demonstration where no crime was committed and where no violence occurred. For some unknown reason the government believed these people must threaten the national security. As a result they were spied on or wiretapped.

If you allow that gaping hole to exist, you have simply destroyed the intent of the fourth amendment and you have given unlimited power to the government under the statute to do wiretapping.

Mr. KASTENMEIER. Yes, what you propose to do is bring all wiretapping into a situation where a warrant is required, whatever its definition?

Senator NELSON. I think that the language of the fourth amendment is so clearly spelled out that there is absolutely no exception under any circumstances. I don't think you can leave any exception.

There should be no problem with "national security" matters because espionage and treason are in fact crimes. They are spelled out as crimes.

If some Government agency believes that there is a matter involving the security of this country which justifies a wiretap, all this proposal says and all the Constitution says is that you must go to a court. It will authorize the wiretap upon oath or affirmation show-

ing probable cause. After all, if the Government does not have to make a showing of probable cause, it has a license to spy on everybody. And there is no way to leave a little crack open without it bursting the whole dam.

Mr. KASTENMEIER. What sanction would you recommend for officials who, notwithstanding the existence of the requirement for a warrant, might nonetheless wiretap, feeling that the reason is such a compelling one that they would resort to both legal wiretapping or illegal wiretapping, similar to the "plumbers'" unit?

Senator NELSON. I don't remember what the provisions are, but that is a criminal offense.

Mr. KASTENMEIER. Do you think we ought to concern ourselves especially with government officials who conduct wiretapping unauthorized by law?

Senator NELSON. I don't think that officials are above and beyond the reach of the law. And of course, people can do things illegally and commit crimes and we may not know it. That is one of the reasons that I would want a bipartisan committee to call before it, at least annually, the head of the FBI, look at his records and put him under oath in order to be sure that he doesn't dare perjure himself. I would then call the head of the FBI in New York and Chicago and Los Angeles and put them under oath. Then next I would call the head of the FBI from Milwaukee and Miami and Houston and put them under oath so that at all times you are having a half dozen people under oath respecting the activities of that agency. Congress can thus be assured that somebody who is dishonest and in a position of power is required to testify under oath. Congress can also be assured that there will be additional testimony that might expose the dishonest agent.

I would do that with respect to military intelligence and all other intelligence. I think that gives you a pretty good guarantee.

For example there is no reason for somebody to risk going to jail for the purpose of spying on citizens participating in Earth Day ceremonies in 1970 to express their concern about the deterioration of the environment. Nor is there any reason for the Government to involve the National Council of Churches' meetings, as was testified before Senator Ervin's committee, and listen to the discussion of these very fine people who were doing nothing criminal and who happened not to like the war that we were involved in.

I don't think that anybody is going to risk going to jail in order to spy illegally upon a perfectly decent citizen, particularly since, if there is probable cause that somebody threatens the national security or probable cause that a crime is being committed or probable cause that shows some citizen is involved with a foreign agent, the court warrant would be issued.

And the reason you can't make any exception is that the exception becomes the rule.

Mr. KASTENMEIER. I take it that the scope of your bill is wiretapping, electronic surveillance? Does it also involve other surveillance, common surveillance?

Senator NELSON. This bill is limited specifically to warrantless wiretaps.

Mr. KASTENMEIER. Would that cover electronic eavesdropping?

Senator NELSON. Yes

Mr. KASTENMEIER. But not other forms of surveillance?

Senator NELSON. No, not other forms of this surveillance.

Mr. KASTENMEIER. The examination conducted by the Joint Committee annually, would that be in executive session, in secret session, or would that be public?

Senator NELSON. I think the committee would have to decide that. It should probably be left up to the authority of the committee. There are obvious cases which you don't want to disclose. And really, the purpose is not to disclose for publication in the paper. The purpose is to disclose to the Congress, to the other branch, what is going on so that we are sure the law is complied with.

The details of who might have been surveilled aren't always the important thing so far as publicity is concerned. If there are violations or wholesale violations, obviously the Congress would do something about it and probably disclose it. But if it involved organized crime or things such as that, obviously they wouldn't and shouldn't.

Mr. KASTENEIER. My last question is, I take it you accept the need for wiretapping and electronic surveillance philosophically but only under conditions which you have described, that is, under warrant?

Senator NELSON. Yes, I accept what the Founding Fathers said that upon probable cause under Oath or affirmation presented to a court, that then a warrant may be issued. I think the government needs that. You need to have a neutral party deciding whether or not the Fourth Amendment to the Constitution is being complied with. And I then would want the third branch of the government do its annual oversight to be sure that the other two branches are complying with the Constitution.

Mr. KASTENMEIER. I yield to the gentleman from California, Mr. Danielson.

Mr. DANIELSON. Thank you, Mr. Chairman. And thank you, Senator Nelson. I infer from your answers to Mr. Kastenmeier's questions that you do ascribe to the provisions of the Fourth Amendment which, as I read them, at least would permit wiretapping under certain carefully defined circumstances.

In looking at your three points, the major points of the Surveillances Practices and Procedures Act, I note that you have restricted the bill to wiretapping. As I understand it, you are excluding the implantation of a microphone, for example——

Senator NELSON. No, we include it.

Mr. DANIELSON. Your definitions would include that?

Senator NELSON. Yes, electronic devices of all kinds.

Mr. DANIELSON. All right. You also, however, seem to tie it only to national security reasons, or national security interests.

Senator NELSON. Pardon? I missed the first part.

Mr. DANIELSON. You seem to restrict the authorized wiretapping to national security reasons, or national security interests.

Senator NELSON. No, the other way around; this is aimed at being sure that this vague phrase "national security" doesn't except wiretaps from the provisions of the Fourth Amendment.

Mr. DANIELSON. Then you do not intend to exclude—and let me use the term here for reference "authorized wiretapping"—you do not intend to exclude wiretapping for the purpose of investigating crimes, in other words, again assuming you got the warrant issued upon probable cause and so forth?

Senator NELSON. Title III of the act and the Constitution covers crime. I wouldn't exclude anything.

Mr. DANIELSON. You say you would not exclude anything?

Senator NELSON. No. I think anything involving electronic surveillance, wiretapping—and I am using "wiretapping" in its broadest term—none of that should be excluded from the provisions of the Fourth Amendment.

Mr. DANIELSON. No, that was not the thrust of my question.

Senator NELSON. Oh, I misunderstood.

Mr. DANIELSON. Let me restate it. I would fully agree with you on that. I don't think that there is any way we can, even if we wish, get away from the Constitution, and I don't wish to.

However, on page 8 of your presentation in the next to the last and the last paragraphs, and then again on page 9, in each of your explanations you say the bill can change three principal provisions: first, before one could wiretap American citizens for national security reasons, the Government would have to obtain a judicial warrant; second, before the Government could wiretap a foreign power or its agents, it would have to obtain a warrant; and the like. And you refer to "national security" in each instance.

Do you intend by referring to "national security" to exclude the possibility of a lawful wiretapping for a nonnational security purpose?

Let's say a felony investigation, which does not involve national security, such as an investigation of a kidnapping or extortion or bank robbery or narcotics peddling or some such thing, where would that fit into wiretapping? There is no national security involved, in other words, just criminal law.

Senator NELSON. No, they are covered in title III of the act now.

Mr. DANIELSON. In other words, you do not intend to restrict this to national security?

Senator NELSON. No, what we intend it to do is to cover what is called "national security".

Mr. DANIELSON. Well, I favor that.

Senator NELSON. No, we do not intend it to exclude anything.

Mr. DANIELSON. I thought you meant that but I was not sure from your presentation.

Senator NELSON. Yes.

Mr. DANIELSON. Thank you.

Mr. KASTENMEIER. If the gentleman from California would yield? The premise is that no one denies that for purposes of investigating a crime, a warrant is required for wiretapping. That is presently the law. The exception claimed by those in the Federal Government is in the area of "national security" and a warrant is not required for certain national security matters. And Senator Nelson's bill covers that and says that in that area too, a warrant shall be required.

Mr. DANIELSON. Which I am very pleased to support. However, I can't quite agree with my chairman that no one would disagree. There are many people who feel that there should be no wiretapping almost under any circumstances, including the violations of criminal law.

Mr. KASTENMEIER. The only point I was making is that presently the law requires a warrant for any Federal or State wiretapping. The only exception claimed by the government presently is in the area of national security, and that is the purpose of Senator Nelson's bill, to make sure that that type of tap as well must be authorized by warrant; is that correct?

Senator NELSON. That is correct and that is the only issue involved here that has not been to the Supreme Court. They ruled on what is called "domestic security" and that is covered clearly.

Mr. KASTENMEIER. Yes.

Senator NELSON. But the assertion of the right to a warrantless wiretap as an exception to the Constitution or as not being covered by the Constitution hasn't been to the Supreme Court. I think clearly if it went there, you wouldn't need this statute. If it went there, I am sure there is no way that the Court could logically rule other than that warrantless wiretaps are in fact unconstitutional, that they are prohibited by the Fourth Amendment. But the issue hasn't gotten there and I don't know whether it will.

Mr. DANIELSON. I don't either. But you know when we pass new legislation, it always has an impact on previous legislation, and I think it is a valuable contribution to this record to make it clear.

Senator NELSON. I agree.

Mr. DANIELSON. To make it clear that you are talking only about national security and you do not intend to restrict or in any way limit the existing laws relative to nonnational security wiretapping.

Senator NELSON. You stated it exactly correctly.

Mr. DANIELSON. Which I fully agree should be governed and I hope are governed by the fourth amendment. Thank you so much.

Senator NELSON. Thank you.

Mr. KASTENMEIER. I would like to recognize the gentleman from New York, Mr. Smith. And the Chair should at the outset state that we are pleased to have Mr. Smith here. The Republican members of our subcommittee are in a formal caucus on a very important issue and may be here a bit later, but in any event I am pleased the gentleman from New York could attend.

Mr. SMITH. Thank you, Mr. Chairman. Senator Nelson, thank you very much for coming here today and giving us the benefit of your testimony. You have given us a lot of food for thought and I don't have any questions, but it has been a good presentation, and thank you.

Senator NELSON. Thank you very much, Congressman.

Mr. KASTENMEIER. The gentleman from Massachusetts, Mr. Drinan.

Mr. DRINAN. Thank you very much Senator Nelson, I will reveal my biases immediately by stating that I and some others have filed a bill to abolish all wiretapping. And the preamble says this: "The chance of its misuse outweighs any potential benefits which might otherwise be found in it."

So I assume that you have concluded that *Olmstead* was correctly decided?

Senator NELSON. No, *Olmstead* went the other way. *Olmstead* said the fourth amendment didn't cover wiretapping. I think they were clearly wrong.

Mr. DRINAN. Do you think wiretapping can be permitted at all by the fourth amendment?

Senator NELSON. Pardon?

Mr. DRINAN. In examining the fourth amendment I have great difficulty in understanding how wiretapping of any nature can come within that provision because in the latter part of the fourth amendment, that is quoted on page 5 of your fine testimony, it says that those who want wiretapping must particularly describe the place to be searched and the person or things to be seized.

And I have the fundamental difficulty that the four dissenters in *Olmstead* had, that all wiretapping cannot comply with that particular requirement.

And your testimony says that the Federal Government has to go to a court to get this warrant, but I don't understand how anybody who wants wiretapping can particularly describe the place and the persons or the things to be seized.

Senator NELSON. Of course at the time the fourth amendment was adopted, there were no telephones and hence no wiretaps; but I think that unreasonable searches and seizures cover wiretaps and electronic surveillance. I take it that you are saying that in fact they don't permit it?

Mr. DRINAN. I am saying, Senator, that in the Surveillance Practices and Procedures Act that you have proposed, there is no description or way by which the Federal Government can comply with the fourth amendment. You have included nothing as to how they shall particularly describe the place to be searched and the persons or things to be seized.

And I say that fundamentally they can't do that. If the judge gives them a warrant—and all judges give warrants whenever they are asked—they simply are in violation of the fourth amendment. Now this is my position, and you haven't come to that position, but how would you answer that difficulty?

Senator NELSON. I think the Congressman can make a reasonable argument as he has. But when you go to the court, you have to describe whose conversation you want to wiretap, you have to describe the premises that you want to wiretap, and you have to give the probable cause for the wiretap. You are making a different argument. You are arguing it is a violation to use it at all, even with a court order, correct?

Mr. DRINAN. Yes.

Senator NELSON. And that is a reasonable argument. I don't think the court would uphold it, but then that doesn't mean you are wrong.

Mr. DRINAN. Before it might not. It might be different now.

Senator, is there any empirical evidence that Federal judges will, in fact, be very careful and scrupulous in granting the warrants that are requested?

Senator NELSON. Well, the law requires them, and the bill requires them to be in compliance with the fourth amendment. It is perfectly clear that it is very common, particularly in the lower courts, for

them to just issue a wiretap order upon request. And I suspect that very frequently there is no reasonable probable cause that would stand up if tested.

So you have the law and you have the Constitution violated by failure to require strict compliance with the law.

Mr. DRINAN. And your bill provides no remedy, no sharpening of the standards for Federal courts.

Senator NELSON. Yes, it does. And I commented, as the Congressman may recall, earlier, that we also need the third branch of the government involved. The Constitution says the government has to go to the court and show probable cause. Now you have the executive branch and the courts involved. I have introduced legislation which will now involve the Congress by its annual oversight, perhaps in executive session. By calling representatives of the Government before it, Congress can require those who have requested warrants to justify those requests. Then we can have oversight over the judicial branch and the executive branch to see whether or not they are in compliance with the Constitution and the specifics of this statute.

Mr. DRINAN. But Senator, we really have no oversight over the courts. If they continue to hand out warrants like green stamps as they now do, then the situation will continue despite your bill.

Senator NELSON. The bill requires that the court must require independent evidence to support the assertion of probable cause; but anyway the court doesn't initiate a request. If you have oversight by the Congress of everyone who initiates the requests and you put them under oath and you make them come in and show the jurisfication that they give the courts, we will find out every single year any particular case where they were in violation. Of course, if they didn't have probable cause, the court also was acting in violation of the Constitution. But at least we've got control over part; at least we've got oversight over the activities of the executive branch. And if they continue to violate the law, we will just have to up the penalty.

Mr. DRINAN. They will make another exemption, Senator, on the ground that the enforcement of the law, particularly in national security really requires that we have wiretapping. And I assume on that premise you would say that the Federal Government should be able to get a warrant to intercept and to read the mail going to the Russian Embassy?

Senator NELSON. The court has already ruled on that.

Mr. DRINAN. I know.

Senator NELSON. And the court has ruled that the fourth amendment covers wiretaps in criminal cases and domestic security cases and that you have to present probable cause for it. And they have ruled that wiretaps and electronic surveillance involves unreasonable searches and seizures.

Now what the Congressman I think is saying is that provision ought to be modified.

Mr. DRIAN. Would you say that the Federal Government should have the power to get a warrant to read the mail of Joseph Kraft?

Senator NELSON. Not if there wasn't probable cause.

Mr. Drinan. But if there is probable cause, they can get a warrant to read the mail?

Senator NELSON. Let's not use my friend Joseph Kraft's name. Let's use Mr. X. If there is probable cause to believe that an individual is involved in a treasonous activity with a foreign power and has access to information involving the security of the United States, and that is presented to the court upon oath and affirmation, and the probable cause is clearly demonstrated, then I think under the fourth amendment, and for the protection of the security of the country, the Government should be able to conduct surveillance, wiretaps, and examine the mail. But they have to describe what they seek and why.

Mr. DRINAN. Senator, does your bill really add anything to the law that the *Berger* decision, the *Katz* decision and the *Keith* decision don't already say that the law is?

Senator NELSON. Those decisions did not touch the question of national security.

Mr. DRINAN. No, the *Keith* decision did, eight to nothing. You quote it here.

Senator NELSON. Not national security. Domestic security.

Mr. DRINAN. So you go beyond the Courts decision to a point that they haven't touched?

Senator NELSON. There are no clear distinctions between "domestic" and "national security." The problem is this administration—and it has been violated in the same way in the past—asserts that here is a so-called national security case and therefore we can have a warrantless wiretap. That apparently is what they did in the *Joseph Kraft* case. If the Government says the national security is threatened, whatever that may be, then it asserts that the provisions of the fourth amendment are not applicable.

This bill is limited to making it clear that there is no such thing as a warrantless wiretap described under the umbrella of national security assertion.

Domestic security has been to the Supreme Court, but not national security.

Mr. DRINAN. But Senator, you are putting all of your faith and hope to dispose of this problem in the Federal Courts, are you not? You think that they are going to be tougher. And I am just suggesting that there is no empirical evidence at all from our recent history to suggest that the Federal courts are going to be tougher with prosecutors. They will give the warrants, and we will have the same thing by a different name.

Senator NELSON. The bill specifically requires them to require the submission of independent evidence showing probable cause.

Mr. DRINAN. Is that a new element of the law, though? You said "independent evidence," but already in the United States Code they have to have the equivalent. You are not adding anything to the standards by which Federal judges are to give out warrants.

Senator NELSON. That is incorrect. We are adding the new standard to cover the argument concerning national security. But in addition, and I repeat, you need the third branch to have oversight to be sure that the court does comply.

If the Government comes before this bipartisan committee to discuss a wiretap issue, and it is shown that there was no probable cause, it will be demonstrated that the law has been violated. I don't

think the Federal judges are going to want to be exposed year after year as in violation of the law.

Mr. DRINAN. It will take a lot of years though before we really have oversight and expose them, as you say.

Senator NELSON. I would like to pass the bill next year and then we would have oversight.

If you pass a law, you are going to have oversight. Then the handful of Federal judges, or other judges, who are likely to be careless with the standards will pay more attention to the standards of probable cause or know that they are going to be exposed by a bipartisan committee of the Congress for not upholding their oath of office.

Mr. DRINAN. You have faith in the Congress that we can expose a body of judges. We haven't been too successful, I am afraid Senator.

One last question. You say, for some reason I don't understand, Senator, that this individual who has been wiretapped without his knowledge or consent would be informed 30 days after the unauthorized interception. There is a very large escape clause there. So I think that under present and probably future practices of the Department of Justice, this man or woman would never really know that his phone had been tapped over a period of time.

Why did you use the arbitrary time of 30 days? Why not the next day or the next hour? And don't you think this is going to be subject to terrible abuse; that disclosure of wiretapping is going to be postponed if the Government tells the court that the person being wiretapped is engaged in a continuing criminal enterprise or that disclosure would endanger national security interests? I mean, here we go again, we've heard that before.

Senator NELSON. That is incorrect. And I repeat again, it is also necessary to pass the oversight bill. With respect to the disclosure requirement, the purpose is to let the citizen know that he has been wiretapped and I think he ought to know. However, if it involved a continuing criminal activity, then the court could postpone disclosure upon petition of the Government based on independent evidence. The Government would have to say, "We don't want to expose our wiretap because it is part of organized crime," or the Government may assert national security and explain what it is. The court could then say "All right, we won't disclose it." But again, it is necessary to have legislation that makes all of this come under the oversight of the Congress.

Mr. DRINAN. All right. Thank you, Senator. I still go back to your major fundamental premise. You assume that wiretapping is a useful and a necessary law enforcement device; yet many law enforcing people say that it is not, that it is an unnecessary device, and it is not really useful. I think the burden is on those who would justify electronic wiretaps as necessary for law and enforcement purposes, to justify it. It is a terrible scandal, as you pointed out eloquently here, and I don't think the scandal is going to go away just by shifting it a little bit so that federal judges have that responsibility.

Senator NELSON. Now Congressman, I haven't testified at all about its usefulness or its value. Maybe it is valueless. I have testified only that wiretapping is covered by the provisions of the fourth amendment. As to its merits, it may be quite valueless. I don't know.

Mr. DRINAN. I am saying you assume that it is valuable because you go to all of these precautions.

Senator NELSON. I am sorry, I don't assume that. The courts have said that wiretapping in domestic security cases and criminal matters is covered by the fourth amendment. I am saying that all of this activity is covered by the fourth amendment.

You are making a second argument that it is useless and valueless and that you shouldn't have it at all. That may be true, but I am saying this is the status of the law and I want every wiretap covered by the fourth amendment. That is all I am arguing here today.

Now if the Congressman comes up with legislation that says that this is all valueless and too dangerous an invasion of privacy and ought to be prohibited, then we ought to look at that in hearings and debate it; but that is a different question.

Mr. DRINAN. I hope you will support such legislation in the Senate. Thank you.

Senator NELSON. You get it over to our side, and I might.

Mr. KASTENMEIER. Senator, on behalf of the committee I want to express my appreciation to you for the contribution you have made today and for the legislation you have introduced in this field. Thank you very much.

Senator NELSON. Thank you very much, sir, and gentlemen.

[The documents referred to at p. 15 follow:]

STATEMENT BY GAYLORD NELSON, A U.S. SENATOR

The time is long past due for Congressional action to check the dangerous abuses of government wiretapping and other surveillance activities. Indeed, continued inaction by Congress in this area would be inexcusable.

The need for action, and therefore the importance of this subcommittee's inquiry, are clear. Uncontrolled government wiretaps and other surveillance activities constitute an intolerable threat to fundamental constitutional rights and liberties. Individual freedom—the cornerstone of our democratic system—is but an illusion in a society where the government can invade an individual's privacy at will.

Until recently, most of the public did not appreciate the inherent dangers of government snooping. Now the public understands that government snooping poses a real threat to everyone, regardless of his or her station in life. Now 77% of the public favors legislation to curb the abuses of government wiretapping and spying.

The explanation for this shift in public opinion is easy to understand. The Watergate scandals and other events have underscored the dangers of government snooping in a dramatic fashion.

Hearings by the Senate Watergate Committee and other Congressional bodies, as well as reports by various periodicals, exposed in sordid detail how the government could and did invade the privacy of law-abiding individuals. Reference to just a few recent examples is sufficient to illustrate the magnitude of dangers of government snooping:

On April 14, 1971, it was revealed that the FBI had conducted general surveillance on those who participated in Earth Day celebrations in 1970. These activities involved tens of thousands of citizens, state governors, representatives of the Nixon administration, and members of Congress. As the one who planned that first Earth Day, I cannot imagine any valid reason for spying on individuals exercising their constitutional rights of speech and assembly in a peaceable manner. There is still no satisfactory explanation of the surveillance. Nor is there any guarantee it could not be repeated in the future.

A 1973 Senate subcommittee report detailed the extensive spying secretly conducted by 1500 agents of the U.S. Army on more than 100,000 civilians in the late 1960's. This surveillance was directed principally at those suspected of engaging in political dissent. No one in the Congress knew about this

spying. No one in the executive branch would accept responsibility for it. Again, there is no guarantee that this sorry episode could not be repeated. In fact, a Senate committee learned recently that in the last three years—after the administration assured the public that the military would no longer spy on civilians—the U.S. Army has maintained numerous surveillance operations on civilians in the United States. And an article in *The New Republic* magazine of March 30, 1974 detailed the U.S. Army's use of wiretaps, infiltrators, and other surveillance techniques to spy on American citizens living abroad who supported the presidential candidacy of George McGovern. The Army's spying, was reportedly so extensive that it even intercepted a letter from a college libarian in South Carolina who requested information about a German publication:

On December 5, 1973, Retired Rear Admiral Eugene LaRoque revealed the existence of a secret unit in the Pentagon which engages in the same kind of activities conducted by the White House "plumbers";

Testimony before the Senate Watergate Committee and the Senate Judiciary Committee documented White House efforts to use confidential tax returns of thousands of individuals to spy on and harrass its "enemies."

For many years Constitutional authorities and other citizens have repeatedly expressed alarm over the rapidly expanding practice of governmental invasions of privacy by wiretapping, data collection, and other forms of surveillance. In 1967 I made a lengthy speech on the floor of the Senate on this issue and in 1971 introduced legislation to establish a joint congressional committee to control government snooping. In this session of Congress I have introduced three separate bills designed to remedy the abuses of government spying. One of these measures—a bill to prohibit the use of wiretaps without approval of a a judicial warrant in so-called "national security" cases—has been introduced in the House by the Chairman of this subcommittee.

Because this last bill, entitled the "Surveillance Practices and Procedures Act of 1973," is presently before the subcommittee, the remainder of this testimony will be devoted to a discussion of it.

The bill is a direct response to wiretap abuses in so-called "national security" cases. Last May it was revealed that in 1969 the White House by-passed established procedures and authorized wiretaps on the telephones of seventeen government officials and newspapermen. The purported basis of these "taps" was a concern that sentitive information was being leaked to reporters by government officials. The government, however, did not obtain a judicial warrant before installing the taps. The government alone decided when it would tap and for how long.

Subsequent investigation showed that some of the government officials tapped did not have access to sensitive information. It was also learned that two of the taps were maintained after the individual involved had left government service and joined the presidential campaign staff of Senator Muskie. In none of the cases was the individual suspected of having violated the law.

These were not isolated incidents. Warrantless taps based on so-called "national security" reasons were placed on the telephones of newspaper columnist Joseph Kraft in 1969 and in 1971 on friends of a Navy yeoman suspected of passing sensitive information to the Joint Chiefs of Staff. Again, none of these individuals were even suspected of having violated the law.

The use of so-called "national security" taps, however, has not been confined to the present administration. Democratic and Republican administrations since the 1930's have used such taps to spy on law-abiding individuals. Various government reports indicate that since that time thousands of individuals have had their telephone conversations intercepted for so-called "national security" reasons.

From the very beginning, those sensitive to civil liberties recognized the dangers of warrantless wiretaps. Such taps enable the government to exercise unchecked and unreviewed power over the individual. There is no opportunity for a court, the Congress, or the public to demonstrate that the taps are unreasonable. For this reason, Supreme Court Justice Oliver Wendell Holmes called them "dirty business." In my view, such taps are also unconstitutional.

To understand the basis of this opinion it is necessary to examine the language and judicial interpretation of the Fourth Amendment. That amendment states quite simply that:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searchers and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

One need not be an historian or a lawyer to understand the essential purpose of this amendment. It is intended to protect the individual's privacy from unreasonable invasions by the government. To afford this protection, the amendment contemplates that a neutral court—not the government—will determine whether any search and seizure planned by the government is reasonable. Otherwise the government would be both advocate and judge of its own case.

The Fourth Amendment thus limits the power of the government. Like the other amendments in the Bill of Rights, it reflects the Framers' intention that individual liberty, rather than unrestrained governmental power, be the hallmark of our political system. In his dissent in the 1928 Olmstead case Supreme Court Justice Louis Brandeis articulated the importance of the Fourth Amendment in our scheme of government:

"The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions, and their sensations. They 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." [Emphasis added].

The Fourth Amendment's protections apply to all government searches and seizures. No exception is made for national security cases or any other kind of circumstance. The absence of any expressed exceptions, moreover, cannot be interpreted as an oversight or a failure of the Founding Fathers to appreciate future developments in which world affairs would be overshadowed by the nuclear sword of Damocles.

When the Constitution was drafted in 1787, our country was only 11 years old. The new American citizens had recently concluded a long war with England to preserve their country's independence. That independence was not entirely secure. The threat of foreign attack and subversion remained ever present. Despite the existence of this treat, the Founding Fathers adopted the Fourth Amendment and made no exception to its application.

In the 1967 *Berger* and *Katz* cases, the Supreme Court held that the Fourth Amendment applies to wiretapping for criminal purposes. In effect, these decisions required the government to obtain an approving judicial warrant before it could install a wiretap in a criminal investigation.

In the 1972 *Keith* case the Court, by an 8-0 vote, decided further that the government could not wiretap individuals without a judicial warrant even when the individual's activities threatened the nation's "domestic security." Again, the Court made clear that wiretaps must adhere to the safeguards delineated by the Fourth Amendment:

"Though physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed, the broader spirit now shields private speech from unreasonable surveillance."

The Supreme Court has not yet decided whether the Fourth Amendment's protections apply to cases involving the intelligence activities of foreign powers and their agents. In the *Keith* case, the Court stated explicitly that it did not consider those situations where American citizens have a "significant connection" with foreign powers and their agents.

Because the Court has not ruled on these "national security" taps, the present administration maintains that it may install warrantless wiretaps in certain situations. In a September 1973 letter to Senator William Fulbright, Chairman of the Senate Foreign Relations Committee, then Attorney General Elliot Richardson stated that the administration would continue to install warrantless wiretaps against American citizens and domestic organizations if the administration believes their activities affect "national security" matters.

Mr. Richardson's comments apparently still reflect administration policy. Last January the Justice Department reported that it had authorized three warrantless wiretaps for national security reasons—an average week's quota according to the department. The department did not explain to any neutral party the justification for the taps or identify the subjects of the taps.

The continued use of warrantless wiretaps for so-called "national security" reasons underscores the need for Congressional action. People in our country should not be afraid to speak to one another on the telephone, never knowing whether the government is listening or how the government might use any information obtained. Every citizen should be assured that the privacy of his or her telephone conversations will not be invaded unless a neutral court first determines that the invasion is justified.

The Surveillance Practices and Procedures Act is designed to provide that assurance. The bill includes three principal provisions.

First, before it could wiretap American citizens for national security reasons, the government would have to obtain a judicial warrant based on probable cause that a specific crime has been or is about to be committed. This provision would thus protect an individual's privacy against unjustified national security wiretaps.

Second, before the government could wiretap a foreign power or its agents, it would have to obtain a judicial warrant based on the belief that the tap is necessary to protect national security interests. The warrant standards for foreign powers and their agents would thus be less rigorous than those required for American citizens. This warrant requirement will in no way undermine the government's ability to protect against foreign attack or subversion; the government will be able to wiretap foreign powers and their agents any time there is a need for such surveillance.

The justification for this second warrant procedure is plain. The government's desire to wiretap should be reviewed by a court. There should be no exceptions. Otherwise the exceptions may be stretched to sanction an unreasonable invasion of an individual's privacy—a situation which would violate the rights and liberties guaranteed under our Constitution.

Third, every American citizen wiretapped would be informed of the surveillance within 30 days after the last authorized interception. This provision would assure every wiretapped American citizen the opportunity to protect against violation of his or her constitutional rights. The disclosure of the wiretap could be postponed however, if the government satisfies the court that the person wiretapped is engaged in a continuing criminal enterprise or that disclosure would endanger national security interests.

The need for legislation such as this should be beyond dispute. Warrantless wiretaps—whether for "national security" reasons or other purposes—pose a grave danger to individual rights of speech and privacy. Such taps invest the government with an absolute power over the individual. They enable the government to pry into an individual's private affairs without justification. They foster the reality of an Orwellian state in which the government becomes a monster to be feared rather than a servant to be trusted.

That is not the kind of government envisioned by our Founding Fathers. The underlying and fundamental premise of our Constitution is that all government power is limited by checks and balances. This is no less true of the government's power to protect "national security." That power is not so absolute that it can excuse infringements of the right to privacy and other constitutional liberties. It would indeed be ironic if the government could invoke "national security" to violate those individual freedoms which the government is obligated to defend.

The public apparently agrees that invocation of "national security" cannot excuse violations of constitutional rights and liberties. A recent Harris opinion poll found that 75% of the public believes that "wiretapping and spying under the excuse of national security is a serious threat to people's privacy."

More than 20 years ago, Justice Felix Frankfuter voted with a majority of the Supreme Court to condemn as unconstitutional President Truman's seizure of the steel mills, an action which that President also tried to justify in terms of "national security." In explaning his vote, Justice Frankfuter observed that:

"The accretion of dangerous power does not come in a day. It does come, however slowly, from the generative force of unchecked disregard of the restrictions that fence in even the most disinterested assertion of authority."

The observation is equally true of warrantless wiretaps in so-called "national security" cases. Over the past few decades, the use of these taps has generated an unchecked power in the executive branch. The danger has now been exposed. In wiretapping, as in other matters, unchecked power can be and often is exercised in an arbitrary and abusive fashion.

It is not a question of good faith. Even the best of intentions can lead individuals—and their government—astray. If Congress wants to insure respect for constitutional limitations and constitutional liberties, it should not rely on the good will of government officials; it should enact legislation which defines clearly the government's obligations and the individual's rights. This is at least one lesson of Watergate. Time will tell how well Congress has learned the lesson.

Section Analysis of the Surveillance Practices and Procedures Act of 1973—S. 2820

SECTION 1

This section identifies the bill as the "Surveillance Practices and Procedures Act of 1973."

SECTION 2

This section consists of findings and declarations by Congress. It is stated that recent events have exposed abuses by governmental agencies and departments when engaging in certain surveillance practices, including the use of wiretaps. It is stated further that these abuses have undermined and/or threatened the individual's constitutional right to privacy and other constitutional rights and liberties. Because of these past violations of constitutional rights and liberties, and because the possibility of future violations has rightly aroused public concern, it is declared that Congress should establish practices and procedures so as to reconcile the interest in protecting constitutional rights and liberties with the interest in enabling the government to execute its investigative and law enforcement responsibilities. The section concludes that the need for these practices and procedures is particularly acute in cases involving the use of wiretaps by the government.

SECTION 3

This section amends section 2510 of title 18, United States Code, by adding a definition for the term "foreign agent." A foreign agent is defined as an individual who is not an American citizen, whose first allegiance is to a foreign power and whose activities are intended to serve that foreign power and to undermine the security of the United States.

SECTION 4(a)

This subsection amends subsection 2511(3) of title 18, United States Code. It empowers the President to authorize wiretaps against foreign powers and their agents when necessary to protect the nation against actual or potential attack or other hostile acts, to obtain foreign intelligence information essential to the security of the United States, or to protect national security information against foreign intelligence activities. In authorizing these wiretaps, the President must adhere to the procedures delineated in section 2518A (described below).

Comment.—Read in conjunction with section 2518A, this subsection requires the President to obtain a judicial warrant before wiretapping foreign powers and their agents. The warrant must be based on evidence, establishing probable cause, that the information derived from the wiretap will serve at least one of the three national security purposes described above.

Under the present wording of section 2511(3), both the government and numerous courts have maintained that the government can conduct wiretaps

without a judicial warrant if the information sought would, in the government's eyes, serve one of the three national security purposes. (See, for example, *United States* v. *Brown*, 484 F.2d 418, 426 (5th Cir. 1973; *United States* v. *Clay*, 430 F.2d 165, 171-72 (1970), *rev'd on other grounds* 403 U.S. 698 (1971).)

These warrantless wiretaps, however, often pose a fundamental danger to the individual rights and liberties guaranteed by our Constitution. Foremost among these threatened rights and liberties are those protected by the Fourth Amendment. That amendment provides that:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The amendment thus protects the individual's privacy from unreasonable invasion by the government. To protect individual privacy, the amendment contemplates that a neutral court or magistrate—not a government intent upon pursuing an investigation—must determine whether any search planned by the government is reasonable. (*Shadwick* v. *City of Tampa*, 407 U.S. 345, 354 1972); *Johnson* v. *United States*, 333 U.S. 10, 13-14 (1948).)

The Supreme Court has made clear that the amendment's "protection reaches all alike, whether accused of crime or not, and the duty of giving it force is obligatory upon all." (*Weeks* v. *United States*, 232 U.S. 383, 391 (1914).) Even foreign agents engaged in espionage enjoy some protection under the Fourth Amendment. (*Abel* v. *United States*, 362 U.S. 217 (1960).)

The greatest dangers of warrantless wiretaps for so-called "national security" reasons are to the constitutional rights and liberties of American citizens. Reports by congressional committees and others have demonstrated that such wiretaps were often by the government to engage in surveillances of American citizens whose activities bore no reasonable relationship to this nation's security.

These abuses underscore the need to have a neutral court review *all* "national security" wiretaps to insure that they are used for lawful purposes. The Fourth Amendment does not except "national security" cases from the scope of its protection. Nor should there be any exception for "national security" cases. Otherwise it is possible—if not likely—that the power to conduct warrantless wiretaps can be used again to violate the constitutional rights and liberties of American citizens. Section 4(a) of the bill minimizes that possibility by requiring the government to obtain an approving judicial warrant before it can wiretap foreign powers or their agents.

The warrant procedure does not impose any unconstitutional restriction on the President's constitutional powers as Chief Executive, as Commander-in-Chief of the Armed Forces, or as the Nation's chief foreign policy officer. To begin with, the fundamental premise of our Constitution is that there are no absolute powers in any branch of the government—all power is "fenced about." (Berger, *Congress* v. *The Supreme Court* 8-15 (1969).)

Congress has the Constitutional power to define the limits of the President's wiretap authority. In the *Keith* case (*United States* v. *United States District Court*, 407 U.S. 297 (1972)), the Court stated explicitly that Congress has the power to establish standards under which wiretaps could be authorized—even if those standards restricted the President's powers. (See esp. 407 U.S. at 338, n.2, White, J., concurring opinion.) No court has held to the contrary. Indeed, in sustaining presidential authority to conduct warrantless wiretaps, courts have placed primary reliance on *United States* v. *Curtiss-Wright*, 299 U.S. 304 (1936), and *Chicago & Southern Air Lines, Inc.* v. *Waterman Steamship Co.*, 333 U.S. 103 (1948)—two cases which involved authority delegated to the President by laws enacted by Congress. (See *Youngstown* v. *Sawyer*, 343 U.S. 579, 635, n.2 (1952) (Jackson, J., concurring opinion.) Thus, the courts have not upheld the President's powers to exceed limitations imposed by Congress.

(b) This subsection deletes the second sentence of subsection 2511(3), title 18, United States Code. That sentence states that nothing in the subsection shall limit the President's authority to take measures which he deems necessary to protect the government from violent overthrow or other clear and present dangers.

Comments.—This second sentence is ambiguous and, in light of the clarifying provisions of this bill, unnecessary. The ambiguity derives from the fact that the sentence does *not* confer or recognize any presidential power; it merly states that *if* the President has certain inherent constitutional powers, subsection 2511(3) will not disturb that power (*Keith, supra*, 407 U.S. at 303–308.)

From this construction, some individuals have maintained that the second sentence might tolerate the President's authorization of warrantless wiretaps against American citizens and others whom the government believes pose a threat to the nation's security.

The provisions of this bill make clear, however, that government cannot use warrantless wiretaps under any circumstance. The bill also provides that wiretaps to protect national security can be authorized by a court only when certain criteria are satisfied. (See Secs. 4(a) and 5(a).) In view of this clarification, and since the second sentence does not constitute an affirmative grant of power, it should be deleted.

(c) This subsection amends subsection 2511(3) of title 18, United States Code, so that information obtained from foreign power or foreign agent wiretaps cannot be used in criminal proceedings but can be used in civil proceedings against foreign agents.

Comment.—All aliens—even those engaged in espionage—enjoy Fourth Amendment protections in at least criminal matters. (*Abel, supra.* See *Weeks, supra.*) Therefore, if the government wishes to use wiretap information in a criminal prosecution, it must follow the stricter standards delineated in section 5 of the bill. However, the information gained from foreign power or foreign agent wiretaps could be used in deportation proceedings or other civil proceedings. (*Abel*, 362 U.S. at 237.)

SECTION 4A

This section amends section 2516, title 18 of the United States Code to remove "national security" crimes from the list of crimes for which a wiretap could be authorized under section 2518 or title 18.

Comment.—This section is purely a technical one to separate "national security" crimes from other crimes and make them subject to the procedures of section 2518A as delineated in section 5(b) of the bill.

SECTION 5(a)

This section creates a new section, (2516A), in title 18, United States Code. The section provides that the Attorney General, or a specially designated Assistant Attorney General, may seek court authorization for a wiretap pursuant to section 2518A when (1) there is probable cause to believe a party has committed, is committing, or is about to commit a specific "national security" crime; and (2) the wiretap sought will probably provide evidence concerning the commission of that crime.

Comment.—This subsection permits the government to obtain court authorization for a wiretap when there is probable cause to believe that the wiretap will produce evidence concerning the commission of a crime. This subsection does not in any way limit the President's power to obtain court authorization under a less rigorous standard when the subject of the wiretap is a foreign power or foreign agent. (See Sec. 4(a).)

Subsection 5(a) merely codifies the protections afforded to individuals under the Fourth Amendment. That amendment prohibits government searches and seizures which are unreasonable. A long line of Supreme Court decisions has held that in most circumstances a search must be supported by a warrant in order to be reasonable. (*Coolidge* v. *New Hampshire*, 403 U.S. 443 (1971); *Vale* v. *Louisiana*, 399 U.S. 30, 34-35 (1970); *Chimel* v. *California*, 395 U.S. 752, 762 (1969); *Camara* v. *Municipal Court*, 387 U.S. 523, 528-29 (1967); *Chapman* v. *United States*, 365 U.S. 610, 613-15 (1961); *Johnson* v. *United States*, 333 U.S. 10, 13-14 (1948); *Agnello* v. *United States*, 269 U.S. 20, 32 (1925).) Moreover, in most cases the warrant must be based on probable cause that a crime had been or was about to be committed. (*Brinegar* v. *United States*, 338 U.S. 160, 175-76 (1949); *Husty* v. *United States*, 282 U.S. 694, 700-01 (1931); *Dumbra* v. *United States*, 268 U.S. 435, 439, 441 (1925); *Boyd* v. *United*

States, 116 U.S. 616 (1886). See Lasson, *The History and Development of the Fourth Amendment to the United States Constitution*, 106-121 (Da Capo Press 1970).) As the Supreme Court stated in *Berger* v. *New York*, 338 U.S. 41, 59 (1967), "The purpose of the probable cause requirement of the Fourth Amendment [is] to keep the state out of constitutionally protected areas until it has reason to believe that a specific crime as been or is being committed. . . ." Noncriminal warrants have been sanctioned only for social welfare purposes, such as in housing inspections. (*Camara, supra.*)

The Fourth Amendment protections also apply to invasions of privacy achieved through wiretapping. (*Berger, supra; Katz* v. *United States*, 389 U.S. 347 (1967).) Under these decisions, the government must obtain a warrant before it can wiretap an individual's telephone.

The Supreme Court also held, by a unanimous 8-0 vote, that the government cannot wiretap without a warrant even when the object is to gather intelligence about individuals whose activities threaten "domestic security." In fact, the Court stated that the warrant requirement is even more important when the real object of the wiretapping is intelligence-gathering. In such cases the government may have a tendency to view as "security threats" those who are critical of government policies. According to the Court, the judicial warrant would help insure that intelligence-gathering does not become an excuse for the government to suppress or punish constitutionally-protected speech:

"The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society." 407 U.S. at 314. See *Stanford* v. *Texas*, 379 U.S. 476 (1965).

The Court reserved judgment though, for those situations where American citizens have a "significant connection" with foreign powers or their agents.

The Fourth Amendment's protections against wiretapping should not be suspended merely because the citizens' activities may involve foreign intelligence activities or otherwise affect "national security." As noted above, the amendment itself does not provide an exception for cases involving "national security." Indeed, many thoughtful individuals have declared that no exception can be made for national security cases. In arguing that the Fourth Amendment's protections apply to national security cases, Supreme Court Justice William O. Douglas stated that "there is, so far as I understand constitutional history, no distinction under the Fourth Amendment between types of crimes." (*Katz*, 389 U.S. at 360 (concurring opinion).)

Whatever the interpretation placed on the Fourth Amendment, however it is clear the Congress has the constitutional power to establish reasonable standards for authorizations of wiretaps. (*Keith, supra; Katz, supra.* See generally *Youngstown, supra*, 343 U.S. at 587, 589, 645-46.) The provisions of section 5(a) are reasonable and are consistent with the letter as well as the spirit of the Fourth Amendment.

(b) This subsection establishes a new section 2518A in title 18, United States Code. This new section, in turn, delineates a procedure by which the government can obtain a court warrant for a wiretap in a case concerning "national security." Essentially, the procedures parallel those contained in existing law for wiretaps for domestic crimes. (18 U.S.C. § 2518.) In certain areas, the new section 2518A includes new provisions which eliminate many of the constitutional infirmities and practical problems of existing procedures. (It should be remembered that the Supreme Court has not yet ruled on the constitutionality of existing wiretap procedures.) Generally, the standards incorporated within section 2518A conform with the guidelines issued by the Supreme Court in *Berger, supra*, and refined in subsequent cases.

(b)(1) This subsection provides that applications for an order authorizing a wiretap under title section 2511(3) or section 2516A can be made to a judge of competent jurisdiction. The subsection provides further that in orders involving application of section 2511(3)—wiretaps on foreign powers or their agents—the application can, at the government's discretion, always be made to a judge sitting on the Federal District Court in the District of Columbia; the section thus enables the government to limit the number of judges who would have access to information relating to the need to wiretap foreign powers or their agents.

The subsection also specifies the information which must be furnished to the judge by the applicant. The information required includes (1) the facts which justify the need for the wiretap, (2) descriptions of the location where the wiretap should be installed, (3) descriptions with as much particularity as is possible of the communications sought to be intercepted, (4) the identity, if known, of the person(s) whose communications would be intercepted, and (5) in cases involving application of section 2516A, the particular crime which has been, is being, or will be committed. (NOTE: In cases involving application of section 2511(3)—wiretaps on foreign powers or their agents—the government need *not* establish that the commission of a crime is involved in order to obtain authorization for a wiretap.)

The subsection specifies further that the applicant must provide information as to why use of a wiretap is more appropriate than some other investigative technique. The applicant must also state the length of time for which the wiretap should be maintained, whether any other applications have been made to wiretap the same location or the same persons and, if so, whether such previous applications were approved. If the application is for an extension of an existing wiretap authorization, the application must state the results obtained or explain the failure to obtain the results sought.

Comment.—With few exceptions, the procedures delineated in the subsection parallel those included in the existing wiretap application procedures. (18 U.S.C. §2518.) To the extent changes are made, they are designed to require greater specificity by the applicant in describing the information sought and the purpose for which such information will be used.

The increased specificity is necessary in order to insure that wiretaps conform with the protection afforded by the Fourth Amendment. That amendment provides that warrant permitting searches by the government shall "particularly [describe] the place to be searched, and the persons or things to be seized." In the words of the Supreme Court,

"The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant."

Marron v. *United States*, 275 U.S. 192, 196 (1927). Accord: *Stanford, supra; Kremen* v. *United States*, 353 U.S. 346 (1957).

The amendment thus seeks to restrict government invasions of individual privacy to the minimum necessary. (See *Silverthorne Lumber Co.* v. *United States*, 251 U.S. 385 (1920).

Wiretaps, of course, pose a special problem. When placed on a particular telephone, they permit monitoring of all telephone conversations, regardless of whether or not the conversation overheard is necessary or even relevant to the purposes for which the wiretap was installed. Wiretaps are, in effect, a broad dragnet which allows government surveillance of all who use the tapped telephone, however innocent or innocuous the use. As Justice Dougles observed in *Keith, supra*, "Even the most innocent and random caller who uses or telephones into a tapped line can become a flagged number in the government's data bank. See *Laird* v. *Tatum*, 1971 Term, No. 71-288." (407 U.S. at 326.) Indeed, litigation in wiretap cases has demonstrated that use of wiretaps results in government surveillance of vast numbers of irrelevant conversations. (See, for example, *United States* v. *La Gorga*, 336 F. Supp. 190, 195-97 (W.D.Pa. 1971); *United States* v. *Scott*, 331 F. Supp. 233 (D.D.C. 1971); *United States* v. *Sklaroff*, 323 F. Supp. 296 (C.D. Fla. 1971).) For this reason, the Supreme Court has emphasized the special precautions a court should take before approving any wiretaps:

"The need for particularity and evidence of reliability in the showing required when judicial authorization of a search is sought is especially great in the case of eavesdropping. By its very nature eavesdropping involves an intrusion on privacy that is broad in scope. As was said in *Osborn* v. *United States*, 385 U.S. 323 (1966), the 'indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments and imposes a heavier responsibility on this Court in its supervision of the fairness of procedures . . .' At 329, n. 7."

Berger, 388 U.S. at 56.

In other words, unnecessary invasions of individual privacy cannot be entirely justified by reference to some pressing government need. As the Supreme Court stated in *Berger, supra*, "we cannot forgive requirements of the Fourth

Amendment in the name of law enforcement." (388 U.S. at 62.) Nor can those requirements be forgiven in the name of "national security." (See *United States* v. *Brown*, 484 F.2d 418, 427 (1973) (Goldberg, J., concurring opinion).)

Therefore, in view of these special problems related to government searches accomplished through wiretaps, care should be taken to insure that the invasion of individual privacy is restricted to the minimum necessary. Subsection (b)(1) provides that care.

(b)(2) This subsection states that the judge to whom application is made may require additional materials to support the application. The subsection stipulates further that the judge may not rely on conclusory opinions in ruling that a wiretap is justified under either section 2511(3) or section 2516A.

Comment.—This subsection parallels the existing provision in 18 U.S.C. §2518(2). The stipulation concerning reliance on conclusory opinions is little more than a reaffirmation of the Fourth Amendment's protections. The amendment sanctions searches supported by a warrant based on probable cause. The probable cause requirement—if it is to afford any real protection for individual privacy—cannot be satisfied by a government official's mere assertion that the wiretap is justified. (*Giordenello* v. *United States*, 357 U.S. 480 (1958); *Byars* v. *United States*, 273 U.S. 28 (1927). See *Aguilar* v. *Texas*, 378 U.S. 108, (1964).) The government must be required to show wtih some independent evidence that its opinion is not mere conjecture but grounded in fact. Otherwise wiretap procedures could sanction the kind of unreasonable searches prohibited by the Fourth Amendment.

(b)(3) This subsection provides that a judge may authorize a wiretap within the territorial jurisdiction of his court. The subsection provides further that if, in cases involving foreign powers or their agents, application has been made to a judge in the Federal District Court for the District of Columbia (see subsection (b)(1) above), the judge may authorize a wiretap anywhere within the territorial jurisdiction of the United States. In either case, authorization may be granted only if the judge determines that (1) there is probable cause to believe that the information sought will serve one of the purposes set forth in section 2511(3) or section 2516A; (2) there is probable cause to believe that the communications to be intercepted will provide the information sought; (3) the wiretap is the most appropriate investigative technique by which to obtain the information sought; and (4) there is probable cause to believe that the facilities (i.e. telephone) to be intercepted will be used for the communications to be intercepted.

Comment.—This subsection essentially parallels the existing provision concerning authorization of wiretaps. (18 U.S.C. § 2518(3).) The only change is to permit a Federal judge in the District of Columbia to authorize a wiretap anywhere within the territorial jurisdiction of the United States in cases involving application of section 2511(3) (wiretaps on foreign powers or their agents). The reason for this change is explained in the section analysis of subsection (b)(1) of the bill.

(b)(4) This subsection states that each court order authorizing a wiretap shall specify (1) the identity of the person, if known, whose communications are to be intercepted; (2) the location of the facilities to be wiretapped; (3) a description of the communications to be intercepted; (4) the identity of the agency authorized to conduct the interception; and (5) the period of time for which the wiretap is authorized.

Comment.—This subsection parallels existing provisions concerning court orders authorizing wiretaps for domestic crimes. (18 U.S.C. § 2518(4).)

(b)(5) This subsection provides that wiretaps may be authorized for as long as the court deems necessary but in no event longer than fifteen (15) days. The subsection provides further that the judge may authorize an extension of the wirrertap for as long as ten (10) days if the judge concludes that the wiretap still meets the criteria set forth in subsection (b)(3) of the bill. In all cases—*except* those involving wiretaps of foreign powers or their agents under section 2511(3)—this conclusion can be drawn only if the government makes a *de novo* showing that the extension of the wiretap satisfies the criteria delineated in subsection (b)(3).

Comment.—In large part, this subsection parallels existing provisions concerning the duration of wiretaps and the granting of extensions. (18 U.S.C. §2518(5).) Two changes have been made, however.

First, the maximum time for initial wiretap orders is fifteen (15) days instead of thirty (30). Second, except in cases concerning wiretaps of foreign powers or their agents, the bill provides that a wiretap can be extended only if there is a new (*de novo*) showing by the government that the wiretap will continue to meet the statutory criteria.

These changes reflect the concerns expressed by the Supreme Court in *Berger*, *supra*, and in *Katz*, *supra*. In *Berger*, the Court strongly condemned a state statute which allowed wiretaps to be installed for 60 days on a single showing of probable cause by the government. The Court declared that wiretaps of *any* extensive length would be unconstitutional because such lengthy taps amount to general searches prohibited by the Fourth Amendment. (388 U.S. at 57–59.) In *Katz*, the Court again suggested that wiretaps of long duration would run afoul of the Fourth Amendment.

The basis of the Court's concern here is clear. A wiretap permits a monitoring of all telephone conversations, however innocuous. Under this bill, a wiretap would be permitted only after a showing that it will serve a legitimate government purpose. If the information sought is not obtained after a limited period of time (i.e. 15 days), a serious quetsion arises as to whether the wiretap is the kind of unreasonable search prohibited by the Fourth Amendment. Resort to the courts should be required at that point to insure that the wiretap still satisfies the statuory crieria defined in subsection (b)(3). Moreover, it should not be enough for the government to simply request an extension of the wiretap. Otherwise a single showing of probable cause could justify maintenance of a wiretap on a law-abiding citizen for an indefinite period of time—a result violative of the Fourth Amendment.

The considerations are somewhat different in situations involving surveillance of foreign powers or their agents. Unlike most situations involving American citizens and others, foreign intelligence wiretaps often include lengthy surveillances of embassies and those whose status as a foreign agent is clear.

These kinds of wiretaps should not be discouraged when they are designed to serve a legitimate public purpose. Consequently the government should *not* have to make a new showing to justify an extension of a wiretap on a foreign power or foreign agent.

The Congress has the constitutional power to establish different wiretap standards for different situations. The only requirement is that the different standards be reasonably related to the differences in the situations. As the Supreme Court stated in *Keith*, *supra*.

"Different standards for wiretap orders may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection." 407 U.S. at 322–23.

Under this reasoning, standards for extension of wiretaps on foreign powers or their agents can be constitutional even though those standards are less rigorous than the standards applicable to other situations.

(b)(6) This subsection requires the government to make reports to the authorizing judge concerning the progress of the wiretap. The report shall be made as often as the judge requires.

Comment.—The progress report—which is optional under existing wiretap procedures (18 U.S.C. § 2518(6))—is made compulsory to insure that the judge is kept informed of the progress made and that the wiretap order is implemented in a lawful manner.

(b)(7) This section states that the contents of any wiretap information shall be subject to the requirements of Section 2518(8)(a), a provision concerning the recording and storage of wiretap information. The section also provides that the judge shall seal the orders granted and provide for their safe custody.

Comment.—This section merely provides for the applicability of housekeeping procedures contained in existing law for other kinds of wiretaps.

(b)(8) This subsection provides that any individual—*except* a foreign agent—whose conversations are intercepted by a wiretap authorized under this bill should be furnished a copy of the court order authorizing the wiretap, a transcript of the intercepted conversions, and the dates on which such interception occurred. This information shall be furnished within thirty (30)

days after the last court-authorized interception occurs. In no event, however, need the government disclose the identity of a foreign power or foreign wiretapped pursuant to Section 2511(3). Moreover, the disclosure of the wiretap can be postponed if the government satisfies the judge that the individual tapped is engaged in a continuing criminal enterprise or that disclosure would endanger national security interests. The judge would have the discretion to determine the length of any postponement.

Comment.—Existing law concerning wiretaps for domestic crimes provides that a wiretap must be disclosed only prior to the use of wiretap information as evidence in a legal proceeding. This provision offers little protection for the individual tapped for national security reasons.

In most cases, those wiretapped for national security reasons are not prosecuted in a legal proceeding. (See *Laird* v. *Tatum*, 408 U.S. 1 (1972).) In those cases where prosecution is initiated, the government usually abandons the case rather than disclose the wiretap. (See, for example, Salpukas, "Weathermen Case is Dropped by U.S.," *N.Y. Times*, Oct. 16, 1973, P. 1.). In either case, individuals involved are usually deprived of an opportunity to seek redress in court for violations of their Constitutional rights.

This result conflicts with the original understanding of how constitutional rights would be safeguarded. From the beginning, it was presumed that individuals who were the subject of a government search would learn about it. (*Berger*, 388 U.S. at 60. See Lasson, *The History and Development of the Fourth Amendment to the United States Constitution*, Chapters 3 & 4.) Having knowledge of the government search, to the individual could have his day in court to argue that the search infringed on his rights. In proposing adoption of the Bill of Rights in the first Congress, James Madison acknowledged this fundamental role of the courts in protecting constitutional rights:

"Independent tribunals of justice will consider themselves in a peculiar manner the guardians of those rights; they will be an impenetrable bulwark against every assumption of power in the Legislative or Executive; they will be naturally led to resist every encroachment upon rights expressly stipulated for in the Constitution by the Declaration of Rights."

1 *Annals of Congress* 440 (1789).

This role is equally important in protecting constitutional rights against national security wiretaps. As Circuit Court Judge Goldberg explained in *United States* v. *Brown*, *supra*.

"It remains the difficult but essential burden of the courts to be ever vigilant so that foreign intelligence never becomes a *pro forma* justification for any degree of intrusion into zones of privacy guaranteed by the Fourth Amendment."

484 F.2d at 427 (concurring opinion).

It is beyond dispute, then, that an individual's constitutional rights to privacy and speech can be violated by national security wiretaps. A violation is no less real or dangerous because the government does not prosecute the individual tapped.

It is obviously impractical to provide advance notice of the wiretap to the individual who is the object of the surveillance. As the Supreme Court observed in *Katz*, 389 U.S. at 355, n.16, advance notice might "provoke escape of the suspect or the destruction of critical evidence." Such concerns have little force *after* the wiretap is completed and removed. Therefore, except in "exigent circumstances" (*Berger*, 388 U.S. at 60), an individual should be informed of completed national security wiretaps of his conversations so that there is an opportunity for legal redress even if the government does not prosecute.

Subsection (b)(8) of the bill achieves this constitutional purpose. It provides for disclosure of national security wiretaps after the tap has been removed. Disclosure could be postponed only when the authorizing judge is satisfied that the individual tapped is engaged in a continuing criminal enterprise or that disclosure would endanger national security interests. This discretion for postponement would insure that important national security interests are not compromised unnecessarily.

(b)(9) This subsection provides that any aggrieved person may prevent the use of wiretap information as evidence against him in any legal proceeding if such information was obtained unlawfully or is being used in an unlawful manner. The subsection also provides the government with a right

for immediate appeal to a higher court if the presiding judge should prevent the use of wiretap information.

Comment.—This provision simply parallels existing law concerning the use of information obtained from wiretaps for domestic criminal purposes. (18 U.S.C. §2518(10).) This section is in part a codification of Supreme Court decisions that evidence secured by the government as a result of an unconstitutional search is "poisoned" and cannot be used in a legal proceeding. (*Weeks, supra.* See *Alderman* v. *United States*, 394 U.S. 165 (1969).)

SECTION 6

This section provides for the codification of the bill's two new titles, 2516A (application for wiretaps for national security purposes on those other than foreign powers and their agents) and Section 2518A (procedures for obtaining a court order authorizing a wiretap for national security purposes).

SECTION 7

This section provides that certain information concerning wiretaps authorized under the new Section 2518A shall be reported to the Administrative Office of the United States Courts within thirty (30) days of the last authorized interception.

Comment.—The existing law provides that all wiretaps for domestic criminal purposes must be reported to the Administrative Office of the United States Courts. (18 U.S.C. § 2519(1).) Wiretaps authorized under the new section 2518A also should be reported so that there can be accurate records of all wiretaps. There should be no concern that this reporting requirement will in any way compromise sensitive information. Past experience has demonstrated that any confidential information transmitted to the Administrative Office remains confidential.

[From the Congressional Record, Feb. 4, 1974]

SURVEILLANCE PRACTICES AND PROCEDURES OF 1973—AMENDMENT

AMENDMENT NO. 960

(Ordered to be printed and referred to the Committee on the Judiciary.)

INDIVIDUAL PRIVACY AND THE NATIONAL SECURITY

Mr. NELSON. Mr. President, the time has come to end the wiretapping abuses perpetrated in the name of national security. These national security taps today are not authorized by a judicial warrant. The Government is, therefore, free to determine whom it can tap and when it can tap.

Warrantless taps pose a grave danger to fundamental constitutional liberties. Recent events demonstrate that the individual's right to privacy has been and made continue to be violated by the Government's use of such wiretaps. Often they reflect nothing more than a desire to pry into an individual's private affairs. Generally they are not supported by concrete evidence to justify the invasion of an individual's privacy. And always they escape the scrutiny of the courts, the Congress and the public at large because the Government is not required to disclose their existence unless it prosecutes the individual involved—a rare occurence in the history of national security wiretaps.

Congress should act now to end this intolerable situation. Every American citizen should be assured that his privacy will not be invaded unless a court has determined that the invasion is justified.

Last December I offered a bill (S. 2820) which would provide this assurance. The bill would prohibit the use of warrantless wiretaps against American citizens in national security cases. The basis of this legislative proposal is clear.

The fourth amendments to the U.S. Constitution prohibits Government invasions of a citizen's privacy without a judicial warrant. Supreme Court decisions make clear, moreover, that the fourth amendment protections generally apply to Government wiretaps.

Despite the clear meaning of the fourth amendment, the Government continues to authorize wiretaps without a judicial warrant. A couple of weeks ago

the Justice Department reported that it had authorized three warrantless wiretaps for national security cases.

The danger of warrantless wiretaps is not confined to the criminal and truly subversive elements without our society. Warrantless wiretaps are a serious threat to everyone, regardless of his or her station in life. Many distinguished Americans, for instance, have been among those subject to national security wiretaps.

Those wiretapped in recent years include Dr. Martin Luther King, Jr., who was wrongly suspected om being a Communist dupe in the early 1960's; Joseph Kraft, the syndicated newspaper columnist; 17 newspapermen and Government officials who were suspected of leaking or reporting sensitive information in 1969— despite the fact that some of those tapped did not even have access to such information; congressional aides who knew reporters involved in the publication of the Pentagon Papers; and only last week the Washington Post revealed four more warrantless wiretaps conducted by the White House "plumbers" in 1972 against friends of a White House official suspected of passing information to the Chairman of the Joint Chiefs of Staff of the U.S. Armed Forces.

These and other incidents show that often national security wiretaps have been used to protect an administration from adverse publicity rather than to protect the Nation against foreign attack or subversion.

The abuses of warrantless wiretaps have rightly aroused concern among the public. Numerous opinion polls indicate that more than 75 percent of the people now favor legislation to curb Government power to wiretap.

The vast majority of the public instinctively recognize that lack of control breeds an official state of mind that condones the Government's invasion of a citizen's privacy. This official attitude is a dangerous threat to freedom. It led to Watergate and other illegal acts of political espionage.

It is incumbent upon Congress to adopt measures to prevent future abuses and alleviate public concerns. S. 2820 provides Congress with a timely opportunity to meet its responsibility.

The basic purpose of the bill is to guarantee that the individual's constitutional rights and liberties do not fall prey to national security wiretaps. It would indeed be ironic if the Government's invocation of "national security" could justify a violation of those constitutional rights and liberties which the Government is supposed to make secure.

After the bill was introduced, comments from legal scholars and other authorities throughout the country were solicited by my office. Their responses, as well as the additional materials which they brought to our attention, were considered carefully. That consideration, in turn, has made clear that certain amendments are both necessary and appropriate to insure that the bill strikes a proper balance between constitutional liberties and legitimate national security needs.

Accordingly, I am introducing those amendments today. These amendments effect three basic changes in the bill.

First, before the Government could wiretap American citizens in national security cases, it would have to obtain a judicial warrant based on probable cause that a specific crime has been or is about to be committed. This change would help protect an individual's constitutional rights against national security wiretaps.

Second, before the Government could wiretap a foreign power or its agents, it would have to obtain a judicial warrant based on the belief that the tap is necessary to protect national security interests. The warrant standards for foreign powers and their agents would thus be less rigorous than those required for American citizens. This warrant requirement will not in any way undermine the Government's ability to protect against foreign attack or subversion; the Government will be able to wiretap foreign powers and their agents any time there is a need for such surveillance.

The justification for this warrant procedure is plain. The Government's desire to wiretap should be reviewed by a court. There should be no exceptions. Otherwise the exceptions may be stretched to sanction an unreasonable invasion of a citizen's privacy—a situation which would violate the rights and liberties guaranteed to every citizen under our Constitution.

Third, every American citizen wiretapped would be informed of the surveillance within 30 days after the last authorized interception. This change would

assure every wiretapped American citizen the opportunity to protect against violations of his constitutional rights. The disclosure of the wiretap could be postponed, however, if the Government satisfies the court that the person wiretapped is engaged in a continuing criminal enterprise or that disclosure would endanger national security interests.

These amendments are essential to achieve the bill's stated purposes. Mr. President, I, therefore, ask that the amendments be referred to the Judiciary Committee so that the committee can consider them when it reviews the bill.

I. THE SCOPE OF THE FOURTH AMENDMENT'S PROTECTION

To appreciate the dangers of warrantless wiretaps, it is first necessary to understand the scope of the Fourth Amendment's protection. That amendment provides that—

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

This amendment thus restricts the Government's power over the individual. As James Madison observed, this amendment, as well as the other amendments in the Bill of Rights:

"Limit and qualify the powers of Government, by excepting out the grant of power those cases in which the Government ought not to act, or to act only in a particular mode. 1 *Cong. Journal* 483 (June, 1789)."

In this light, the basic purpose of the fourth amendment is clear. It is designed to protect each citizen's privacy from unreasonable invasion by the Government.

The fourth amendment was borne from the American Colonies' bitter experience with their British rules. The English King's officers—armed with nothing more than a general warrant and a desire to suppress political dissent—frequently entered an individual's home and rummaged through his personal effects. Those warrants, and the indiscriminate searches which they sanctioned, quickly became a subject of dread among the American Colonies. See N. Lasson, "The History and Development of the Fourth Amendment to the United States Constitution," chapter 3 and 4 (1937).

In drafting a constitution to govern their new nation, the American citizens were concerned that there be no resurrection of those indiscriminate searches by the Government. The fourth amendment was, therefore, adopted to meet that justified concern.

The fourth amendment's protection is twofold. On the one hand, it precludes unreasonable invasions of an individual's privacy by the Government. On the other hand, the fourth amendment guarantees that that privacy can be invaded only when there is a judicial warrant based on probable cause. The fourth amendment's twofold protection was aptly summarized in a recent issue of the Arizona Law Review:

"The fourth amendment was intended not only to establish the conditions for the validity of a warrant, but also to recognize an independent right of privacy from unreasonable searches and seizures. Justice Frankfurter, dissenting from the (Supreme) Court's decision in *Harris* v. *United States*, interpreted '(t) he plain import of this (to be) * * * that searches are 'unreasonable' unless authorized by a warrant, and a warrant hedged about by adequate safeguards.' "

"NOTE.—'Warrantless Searches in Light of *Chimel:* A Return to the Original Understanding,' 11 *Ariz. L. Rev.* 455, 472 (1969)."

It is quite clear, moreover, that the fourth amendment's protections were not to be suspended in cases of national security. When the fourth amendment was adopted, our Nation was only 11 years old. Foreign threats to the Nation's newly won independence remained ever present. Yet the fourth amendment provides for no exception to its application. The compelling conclusion is that the amendment should be applicable to all situations, includisg cases involving national security crimes. This conclusion is supported by innumerable constitutional scholars, including Justice William O. Douglas, who has stated:

"There is, so far as I understand constitutional history, no distiction under the Fourth Amendment between types of crimes. *Katz* v. *United States*, 389 U.S. 347, 360 (1967) (concurring opinion)."

Our Founding Fathers, of course, did not contemplate the advent of telecommunications. Consequently, the amendment does not expressly include wiretaps of telephones within the ambit of its protection. But there is no question that the constitutional right to privacy in no less imporant in cases where the Government listens to a telephone conversation than when it physically enters an individual's home.

In the 1967 decision of Berger against New York and Katz against the United States, the Supreme Court held that the fourth amendment therefore generally requires the Government to obtain a judicial warrant before it can wiretap a citizen's phone. In issuing the Katz decision, the Supreme Court made clear that—

"The fourth amendment protects people, not places."

The soundness of the Berger and Katz decisions have been reaffirmed repeatedly by the Supreme Court. See, for example, *Alderman* v. *United States*, 394 U.S. 165 (1969). Most recently, in *United States* v. *United States District Court* (407 U.S. 297 (1972)), commonly referred to as the Keith case, the Court held that the Government could not wiretap American citizens without a judicial warrant—even when the citizens' activities threatened the domestic security of the Nation. Again, the Court made clear that wiretaps must adhere to the safeguards delineated by the fourth amendment:

"Though physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance."

The Supreme Court has not yet decided whether the fourth amendment's protections apply to cases involving foreign powers and their agents. In the Keith case, the Court stated explicitly that it did not consider those situations where American citizens have a "significant connection" with foreign powers and their agents.

Because the Court has not ruled on these "national security" wiretaps, the present administration maintains that it may install warrantless wiretaps in certain situations. In a September 1973 letter to Senator William Fulbright, chairman of the Senate Foreign Relations Committee, then Attorney General Elliot Richardson stated that the administration would continue to install warrantless wiretaps against private citizens and domestic organizations if the administration believes that their activities affect national security matters.

Mr. Richardson's comments apparently still reflect administration policy. A couple of weeks ago the Justice Department reported that it had authorized three warrantless wiretaps concerning national security matters.—See N.Y. Times, January 16, 1974, p. 18, col. 1—The Justice Department did not indicate whether the wiretaps included surveillance of American citizens. And that is precisely the problem of national security wiretaps.

The discretion to determine when such warrantless wiretaps are justified and properly executed has been the sole province of the executive branch. There has been no opportunity for the Congress, a court, or any other public body to examine the exercise of that discretion in order to prevent abuses. The results are not surprising. Warrantless wiretaps have produced and continue to produce the very evils which the fourth amendment was designed to eliminate.

II. THE HISTORY OF WARRANTLESS WIRETAPS

Warrantless wiretaps were first employed early in the 20th century. Almost from the very beginning constitutional scholars and law enforcement officials recognized the serious dangers of warrantless wiretaps. In an early surveillance case, the venerable Justice Oliver Wendell Holmes referred to warrantless wiretaps as "dirty business." *Olmstead* v. *United States*, 277, U.S. 438, 470 (1928) (dissenting opinion.)

In 1931, J. Edgar Hoover, who by then had been FBI director for 7 years, commented that—

"While [the practice of warrantless wiretaps] may not be illegal, I think it is unethical, and it is not permitted under the regulations by the Attorney General."

In 1939 Mr. Hoover wrote to the Harvard Law Review that he believed wiretapping to be "of very little value" and that the risk of "abuse would far outweigh the value."

By 1939, however, pervasive reservations about wiretapping had inspired enactment of a law by Congress. In 1934, Congress passed the Communications Act. Section 605 of that act prohibits the "interception and divulgence" or "use" of the contents of a wire communication. From the moment of enactment, the provision seemed to erect a total prohibition to wiretapping and the use of information obtained from wiretapping. See *Nardone* v. *United States*, 308 U.S. 338 (1939); *Nardone* v. *United States*, 302 U.S. 379 (1937). This, at least, was the interpretation of civil libertarians acquainted with the legislative history. Indeed, subsequent efforts in the 1940's and 1950's to legalize certain kinds of wiretapping were repeatedly rebuffed by those in Congress who feared the consequences which wiretapping would have for civil liberties. See Theoharis and Meyer, "The 'National Security' Justification for Electronic Eavesdropping: An Elusive Exception," 14 Wayne L. Rev. 749 (1968).

On the eve of World War II, however, President Franklin D. Roosevelt became convinced that use of warrantless wiretaps would be necessary to protect the Nation against the "fifth column" and other subversive elements. Roosevelt, therefore, instructed his Attorney General, Robert Jackson, to authorize wiretaps against subversives and suspected spies.

But Roosevelt was not insensitive to the risks which wiretapping could have for constitutional rights and liberties. In a memorandum to Jackson dated May 21, 1940, Roosevelt indicated that he was aware of section 605 and had read the Supreme Court's interpretive decisions. Roosevelt basically agreed with the restrictions against wiretapping:

Under ordinary and normal circumstances wiretapping by Government agents should not be carried on for the excellent reason that it is almost bound to lead to abuse of civil rights.

Roosevelt consequently instructed Jackson—

"To limit these investigations so conducted to a minimum and to limit them insofar as possible to aliens."

Roosevelt's sensitivity to the dangers of warrantless wiretaps did not necessarily rescue their legality. Many legal scholars have suggested that until enactment of title III of the Omnibus Crime Control and Safe Streets Act of 1968, all wiretapping was illegal. See, for example, Navasky and Lewin, "Electronic Surveillance," in hearings before Senate Subcommittee on Administration Practices and Procedures (U.S. Senate, 92d Cong., 2d sess., pp. 173–74, 180 (June 29, 1972). Theoharis and Meyer, for instance, observed that until 1968:

"All wiretapping violated the absolute ban of section 605 of the Federal Communications Act of 1934, and all other electronic eavesdropping which resulted in trespass of a constitutionally protected area was prohibited."

The questionable legality of wiretapping did not deter its use after World War II. In the 1950's and the 1960's the Government's reliance on warrantless wiretaps mushroomed. No precautions were taken, though, to minimize the dangers to civil liberties recognized by Roosevelt. Concern for "national security" consequently led to the use of warrantless wiretaps against political dissidents—including Dr. Martin Luther King, Jr., who was wrongly suspected of being an unwitting dupe of the Communists.

The use of warrantless wiretaps had become a monster with its own momentum. Even the President did not always know the full extent to which such taps were used. Thus, upon learning of the taps on Dr. King and others, President Lyndon Johnson became irate.

On June 30, 1965, Johnson issued a directive placing severe restrictions on the use of warrantless wiretaps. Johnson initially made clear his general opposition to warrantless wiretaps:

"I am strongly opposed to the interception of telephone conversations as a general investigative technique."

Johnson nonetheless ordered that wiretaps be permitted in national security cases—but only with the specific authorization of the Attorney General. Johnson apparently believed, in good faith, that authorization of warrantless wiretaps by the Attorney General would prove to be an adequate safeguard for the individual's constitutional right to privacy and other constitutional liberties.

Sadly, but not unexpectedly, Johnson's belief proved to be illusory. Recent events have demonstrated that warrantless wiretaps—no matter how benign the Government's motives—cannot insure the sanctity of the individual's right to privacy. Reference to the examples cited in my statement of December 17, 1973—S23026—makes this clear:

"On December 5, 1973, Eugene La Roque, a retired rear admiral in the U.S. Navy, revealed that the Pentagon currently has a unit which is authorized to engage in the same kind of surveillance activities conducted by the "Plumbers Unit" in the White House. The purported basis of these activities is a need to protect "national security." Rear Adm. LaRoque emphasized that there is currently no procedure for Congress, the courts, or the public to determine the scope—or lawfulness—of the Pentagon unit's surveillance activities.

"In a report issued in October 1973, a House subcommittee found that certain White House officials invoked national security considerations to make the CIA their "unwitting dupe" in the burglary of Daniel Ellsberg's psychiatrist's offices and in other unlawful surveillance activities.

"Recently it was learned that in 1969 the administration installed warrantless taps on 13 government officials and 4 newsmen for the purported reason that these individuals were leaking or publishing sensitive foreign intelligence information. In virtually all the cases there was little or no concrete evidence to justify the taps. In many cases the evidence shows that the individual tapped did not even have access to such information. Indeed, in at least two cases the taps were continued after the individual had left Government service and had joined the Presidential campaign staff of Senator Muskie.

"In 1969 the White House authorized the burglary of the home of newspaper columnist Joseph Kraft so that a warrantless tap could be installed. The alleged basis for this action was again national security. But there was and is no concrete evidence to establish that Mr. Kraft was acquiring or reporting any information which compromised our national security.

"Testimony before the Senate Watergate Committee revealed that the White House authorized warrantless wiretaps "from time to time" when it was conducting an independent investigation of the publication of the "Pentagon papers" in 1971. The taps were placed on numerous citizens, including aides of Members of Congress, whose only connection with the "Pentagon papers" was a personal relationship with some of the reporters involved. Again, the taps were justified on national security grounds and, again, there was and is no concrete evidence to support the need for the taps.

"In 1970, the White House conceived and drafted a broad plan which proposed warrantless wiretapping, burglary, and other insidious surveillance practices. The staff assistant responsible for the plan started in a memorandum to the President that certain aspects were "clearly illegal." Nonetheless, the plan was approved on the basis of national security, only to be scrapped shortly afterward when FBI Director J. Edgar Hoover objected."

In addition to these abuses, the Washington Post disclosed last week four more warantless wiretaps conducted by the White House "plumbers" in 1972 against American citizens. The presumed basis for these taps was again national security. But there was no involvement of foreign powers or their agents. Nor were the taps in any way necessary to protect our Nation from foreign attack or subversion. The taps were instead justified on the grounds that a White House official was distributing certain information to the Chairman of the Joint Chiefs of Staff of the U.S. Armed Forces. In order to stop this distribution, the "plumbers" believed it necessary to wiretap the official's friends.

These abuses of warrantless wiretaps underscore the wisdom of the fourth amendment's protections. It would be naive to assume that the Government can make a disinterested judgment as to whether a planned search by Government agents is reasonable. The Government cannot properly be worth advocate and judge of its own.

Our Founding Fathers recognized this problem and adopted the fourth amendment. That amendment contemplates that a distinterested court will decide whether searches desired by the Government are reasonable. See, for example, the Keith case; *Coolidge v. New Hampshire*, 403 U.S. 443 (1971). The need for this disinterested judgment is no less necessary in cases involving the national security than it is in other cases. This essential point was advanced eloquently by Justice Douglas in the *Katz* case:

"Neither the President nor the Attorney General is a magistrate. In matters where they believe national security may be involved they are not detached, disinterested, and neutral as a court or magistrate must be. Under the separation of powers created by the Constitution, the Executive Branch is not supposed to be neutral and distinterested. Rather, it should vigorously investigate and prevent breaches of national security and prosecute those who violate the pertinent federal laws. The President and the Attorney General are properly interested parties, cast in the role of adversary, in national security cases. They may even be the intended victims of subversive action. Since spies and saboteurs are as entitled to the protection of the Fourth Amendment as suspected gamblers like petitioner, I cannot agree that where spies and saboteurs are involved adequate protection of Fourth Amendment rights is assured when the President and Attorney General assume both the positions of adversary-and-prosecutor and disinterested, neutral magistrate. 389 U.S. at 359-60 (concurring opinion)."

In short, regardless of how beneficient the Government's intentions, warrantless wiretaps—whether in "national security" cases or in any other kind of case—pose serious dangers to the right to privacy as well as other constitutional rights and liberties.

III. AMENDMENTS TO PROTECT AGAINST WIRETAP ABUSES IN NATIONAL SECURITY CASES

The history of warrantless wiretaps for "national security" cases demonstrates the need for corrective action. For too long Congress has closed its eyes to the abuses of those wiretaps—perhaps in the hope that the country would be better served if implicit trust were placed in the executive branch to safeguard constitutional rights. The history underlying the fourth amendment should have given Congress pause before being so trusting.

But whatever the rationale for past inaction, the Watergate scandals make clear that Congress must act now to insure the preservation of precious constitutional rights—especially the right to privacy. Invocation of "national security" should not enable the Government to wiretap without regard to traditional constitutional limitations. These amendments provide Congress with an opportunity to assure the sanctity of those limitations.

The amendments effect three basic changes in S. 2820, the bill offered last December.

First, before the Government could wiretap American citizens in national security cases, it would have to obtain a judicial warrant based on probable cause that a crime had been or was about to be committed. The crime involved, moreover, would have to be one affecting this Nation's security. Such crimes include those under the Atomic Energy Act, treason, espionage, and sabotage.

This change merely reasserts the traditional safeguards provided by the fourth amendment. That amendment states that the Government cannot invade an American citizen's privacy without first obtaining a judicial warrant based on probable cause. The history of the amendment suggests that, except in certain matters—such as housing inspections—the "probable cause" requirement must relate to the commission of a crime. See, for example, *Wyman* v. *James*, 400 U.S. 309 (1971); *Camara* v. *Municipal Court*, 387 U.S. 523 (1967).

The history of the fourth amendment also underlies the need for prior judicial authorization for national security wiretaps. In United States against Brown, Circuit Judge Goldberg explained the importance of the court's role in supervising such wiretaps:

"It remains the difficult but essential burden of the courts to be ever vigilant, so that foreign intelligence never becomes a *pro forma* justification for any degree of intrusion into zones of privacy guaranteed by the Fourth Amendment. 484 F. 2d 418, 427 (1973) (concurring opinion)."

The Watergate scandals should teach us that the courts cannot carry this essential burden unless prior judicial approval is required for national security wiretaps.

The amendments offered today provide a second basic change: Before it can wiretap foreign powers or their agents, the Government would have to obtain a judicial warrant. This warrant would be issued if the Government satisfies a judge only that the wiretap is necessary to protect the national security. The Government need not establish that the commission of a crime is involved. The standards for foreign power taps, therefore, would be less rigorous than the standards applied for American citizens.

This second change is to insure that the power to wiretap foreign powers is not abused in a manner which infringes on the rights of American citizens. A power to conduct warrantless wiretaps for foreign powers and their agents might enable the Government to violate the constitutional rights and liberties of American citizens. The recent past provides many occasions when legal restrictions on Government wiretapping have been ignored or misinterpreted. Those abuses, in fact, have inspired deep public concern that individual privacy can be violated at any time by Government wiretaps. Public opinion polls reveal that more than 75 percent of the public now favors a curb on the Government's power to wiretap.

Many of those most familiar with foreign power wiretaps share this concern. Former Attorney General Ramsey Clark, for example, recently testified at a congressional hearing:

"Certainly there should be absolutely no use of wiretap or electronic surveillance without a court order under any circumstances . . . Foreign as well as domestic."

Morton Halperin, a former member of Secretary Henry Kissinger's National Security Council staff, is another individual who shares this view.

There should be no concern that a requirement of judicial warrants for foreign power wiretaps will undermine the security of this Nation. Courts will be most responsive to legitimate requests for foreign power taps; as a result, there will be no restriction on the Government's ability to protect the Nation against foreign attack or subversion. Moreover, the implementation of title III of the Crime Control Act—which requires judicial authorization for domestic criminal wiretaps—demonstrates that judges will jealously guard any sensitive information made available to them.

In short, judicial warrants for foreign power wiretaps will have no adverse consequences for this Nation's security. Indeed, former Attorney General Clark has testified that the impact of such warrants on national security "would be absolutely zero."

The third basic change provided by the amendments concerns national security wiretaps on American citizens. Within 30 days after the last authorized interception, the Government would have to disclose the existence of the surveillance to those citizens tapped. This disclosure could be postponed, however, if the Government satisfies the court that the individual involved is engaged in a continuing criminal enterprise and that disclosure would endanger national security interests. This option for postponement would prevent disclosures from undermining the Government's ability to protect the Nation against foreign attack or subversion.

This change again merely codifies the traditional safeguards afforded by the fourth amendment. From the beginning, it was assumed that the courts would protect the individual's right to be secure from unreasonable searches by the Government. In proposing adoption of the fourth amendment and the other amendments in the Bill of Rights, James Madison outlined this role to be played by the courts:

"Independent tribunals of justice will consider themselves in a peculiar manner the guardians of those rights; they will be an impenetrable bulwark against every assumption of power in the Legislative or Executive; they will be naturally led to resist every encroachment upon rights expressly stipulated for in the Constitution by the declaration of rights. 1 *Cong. Journal* 440 (June, 1789)."

The courts could guard the right to privacy in one of two ways. Either the courts could refuse to issue a warrant authorizing a Government search; or the courts could respond to an individual's complaint that the Government had conducted an unconstitutional search.

The latter response of course presumed that the individual would know that the Government had in fact conducted a search. In the early days of our Republic the Government agents would generally knock at the individual's door, present the warrant, and conduct the search. Having knowledge of the search, the individual could complain to a court that the warrant was insufficient—or, perhaps, that the Government executed the search despite the lack of a warrant. This opportunity to complain existed even when the American colonies suffered under British rule. Indeed, if the colonials were not informed of the indiscriminate searches conducted by the British, they would have had no basis to believe that adoption of the fourth amendment was necessary. See N Lasson, "The History and Development of the Fourth Amendment to the United States Constitution," chapters 3 and 4 (1937).

The advent of telecommunications has changed all this. Warrants can be issued and searches conducted without the subject ever learning of them. Unless the Government decides to prosecute the individual tapped, it need not make any disclosure to the individual at any time. For this reason, few of the American citizens tapped for national security reasons in the last few decades have ever learned of the Government's surveillance—even though in some cases it continued for years.

The fourth amendment's protection against Government invasion of individual privacy is weakened if a citizen can be kept ignorant of Government wiretaps. Without knowledge of those wiretaps, the individual is stripped of all opportunity to complain to a court that they have violated his rights. Telecommunications have enhanced considerably the Government's power to snoop on its citizens; telecommunications should not become an excuse to avoid constitutional safeguards.

IV. CONCLUSION

For decades the Government has used warrantless wiretaps to serve its view of the national security. These wiretaps have always posed a fundamental danger to the freedoms guaranteed by our Constitution. The Watergate scandals and other events have exposed that danger in a dramatic and clear fashion.

We should not fail to heed the warning signs. Constitutional provisions empowering the Government to protect the Nation's security were never thought to justify the subversion of individual freedoms afforded by other constitutional provisions. As Judge Ferguson declared in the United States against Smith, a case concerning the use of warrantless wiretaps for national security purposes:

"To guarantee political freedom, our forefathers agreed to take certain risks which are inherent in a free democracy. It is unthinkable that we should now be required to sacrifice these freedoms in order to defend them. 321 F. Supp. 424, 430 (1971)."

Congress cannot and should not tolerate governmental violations of the individual's constitutional right to privacy by wiretaps or any other means. That right to privacy, as well as other constitutional liberties, are the cornerstone of our democratic system. If those rights and liberties are eroded, the very fabric of our constitutional system is imperiled. Congress should, therefore, act now to protect our cherished rights and liberties from abusive national security wiretaps.

[From the Capital Times, Feb. 7, 1974]

WARRANTLESS WIRETAPS

One of the great mysteries of the U.S. Congress is how much speed it can generate to enact dubious proposals into law, while permitting worthwhile legislation to crawl along like refrigerated sorghum.

One of the most ridiculous charades in recent times was the speedy enactment of a daylight saving bill in the middle of the winter as a supposed salve to the energy crisis.

Wisconsin's Sen. Gaylord Nelson has introduced a vitally needed bill aimed at banning warrantless wiretaps for national security purposes. But watch how slowly that the Nelson bill will work its way forward, despite the sordid revelations of the existence of the White House "plumbers" and the Watergate scandal.

In introducing his proposed ban, Nelson said that the security "taps" which are not authorized by judicial warrant often reflect nothing more than a government desire to pry into an individual's private affairs.

It need not be pointed out to the knowledgable that the Fourth Amendment prohibts government invaasion of a citizen's privacy without a judicial warrant: The Supreme Court has made it clear that the amendment's protection extends to wiretapping.

The Nixon administration has taken upon itself the right to violate the Constitution and determine for itself when to order a warrantless wiretap.

"Although the vast majority of the public will never be the object of a tap, they instinctively recognize the lack of control breeds an official state of mind that condones the government's invasion of a citizen's privacy," said Nelson in introducing his proposal. "This official attitude is wrong and dangerous. It led to Watergate and other illegal acts of political espionage."

Revelations that are an outgrowth of the Watergate investigations indicate distressingly that the danger of warrantless wiretaps is not confined to criminal and truly subversive elements within our society. A prime example of the abuse was the tapping of Joseph Kraft, an outstanding syndicated newspaper columnist.

Public opinion polls indicate that more than 75 per cent of the people now favor legislation to curb government power to wiretap.

Nelson's proposed ban is long overdue. We hope it does not get buried in the morass of molasses that seems to entrap other worthwhile proposals.

(Senator Gaylord Nelson has introduced legislation to require the government to obtain court approval before it can wiretap in national security cases. The following editorials discuss the importance of this legislation)

[From the Washington Post, Feb. 9, 1974]

THE PRESIDENT AND PRIVACY

(By Tom Braden)

President Nixon said the other day that "personal privacy is a cardinal principle of American liberty" and that "electronic snoopers have left Americans deeply concerned about the privacy they cherish. The time has come," he added, "for a major initiative."

Coming from a man whose administration has been notable for wiretapping, mail covering, breaking and entering and spying, it was, at first blush, a surprising statement.

But only at first blush. The text reveals that the President wasn't talking about any of these blatant invasions of privacy. He was talking about the accumulation of electronic data on consumers by credit card companies, banks, department stores and other businesses. Without taking anything away from Mr. Nixon's laudable desire to regulate in this area, it still seems necessary to put the question, "What about the Fourth Amendment?"

Just last week, Atty. Gen. William Saxbe said he had initiated three new national security wiretaps. Naturally, Saxbe didn't say who was being wiretapped, whether the taps were being placed upon Americans or foreigners. We may never know. No law requires Saxbe or any subsequent attorney general to tell us. No law requires an attorney general to say what he means by "national security."

Sometimes we are told the numbers. In 1972, testimony before the Senate revealed that 97 "national security" wiretaps were in operation during the year 1970. Since then, we have been given good reason to suspect that a lot of these taps were not placed for the national security but in order to spy on White House enemies. The Watergate investigations have determined that 17 newspapermen and government officials were wiretapped during 1969, and many of the taps were not removed until much later.

Just last week it was revealed that four more wiretaps were conducted by the White House plumbers during 1971 against friends of a White House official.

All of this is in direct contradiction to the Fourth Amendment which declares it "the right of the people to be secure in their persons, houses, papers and effects against unreasonable search and seizure." The Supreme Court has ruled that wiretapping is a "physical entry into a house."

The Founding Fathers never envisioned that a physical entry into a house could be made without a warrant issued upon probable cause and "particularly describing the place to be searched." But not one of these "national security" wiretaps has been authorized by a warrant. Recent attorneys general and Presidents have tapped whomever they wanted to tap. Whether the tap was in the interests of national security or in the interests of politics or in their personal interests has been left to their own consciences.

Thus, Robert Kennedy tapped Martin Luther King—apparently at the insistence of J. Edgar Hoover. Lyndon Johnson is alleged to have tapped members of his Cabinet, and Richard Nixon has widened the "physical entries" to include the press. Under Mr. Nixon, the practice seems to have been so widespread that the President and his attorney general delegated their authorities.

H. R. (Bob) Haldeman, John Ehrlichman and even Henry Kissinger were permitted to make nominations for wiretapping targets, and Mr. Nixon may not have seen the final list of those to be spied upon.

So the President is right when he talks about invasions of privacy as a growing danger, and Sen. Gaylord Nelson (D-Wis.) has introduced a bill which may fix his mind upon the aspect of privacy which he ignored.

Nelson's bill would require the government to seek a warrant before a "national security" wiretap could be authorized or installed. Thus, an independent third party would be able to check upon the power which successive Presidents and attorneys general have used with such frequency.

If the President is really concerned about privacy, he will endorse Nelson's bill.

[From the New York Times, Feb. 17, 1974]

No Warrants, No Taps

(By Tom Wicker)

The Internal Revenue Service's summons for certain records of telephone calls from the Washington Bureau of The New York Times illustrates how a Government that is either careless, callous or expansive can stretch what might appear to be a harmless or even useful power into something different and threatening.

The I.R.S., it seems, has the statutory authority to obtain by civil summons the telephone records of persons it is investigating for tax fraud or delinquency. Most telephone companies have been routinely acquiescing in such summonses.

But the I.R.S. is not investigating The Times or any member of its Washington Bureau—although the I.R.S. also issued a summons for, and received, records of long-distance calls placed from the home telephone of David Rosenbaum, one of The Times' Washington reporters. Instead, it appears that the I.R.S. may be investigating the possible leak of some information from one or more of its employes to Mr. Rosenbaum. Last year, he was working on a story—never published—about a possible I.R.S. investigation of a major contributor to Richard Nixon's re-election campaign.

The point is that the statutes in question do not appear to grant the I.R.S. authority to obtain The Times' or Mr. Rosenbaum's telephone records for the purpose of maintaining its own internal security. Perhaps worse, when first asked about the matter, Donald C. Alexander, Commissioner of the I.R.S., said, "I know nothing of this." Does that mean that lower-level officials can routinely authorize actions that appear to violate the law and offend the First and Fourth Amendments? Since the I.R.S., under challenge, has returned The Times' records, the agency appears to have at least tacitly conceded that it had no legal right to them.

This stretching of authority into areas it was not intended to reach is a relatively old story in government. It lends particular point to a measure introduced by Senator Gaylord Nelson of Wisconsin that would ban all "warrantless" wiretapping and give American citizens a chance to fight back if the Government has its electronic ear on them.

In 1968, Congress authorized the Attorney General to go into court and obtain warrants to tap the telephones of certain persons who could be shown to be criminal suspects. This measure was aimed primarily at organized crime; it did not require the Government to seek warrants before placing taps on persons or organizations for "national security" reasons.

When the Nixon Administration took office, Attorney General John Mitchell began authorizing—without warrants—numerous wiretaps on persons and organizations suspected of threatening "domestic security"; in effect, this "Mitchell doctrine" permitted the Government to tap the phone of anyone it could even remotely link to domestic or national security matters.

In 1972, the Supreme Court, in the so-called Keith case, barred warrantless taps for "domestic security"; but again, the Court did not rule on the question of wiretaps for "foreign intelligence" purposes, which meant that the Government could continue warrantless tapping of foreign embassies, agents of foreign governments and the like. This left a significant loophole in the Fourth Amendment rights of American citizens, who still could be tapped without a

warrant if their activities caused the Government to consider them possible agents or dupes of foreign governments.

In September, 1973, in fact, Attorney General Elliot Richardson wrote Senator J. W. Fulbright that the Government was continuing warrantless tapping of citizens and organizations whose activities it believed could affect national security. His successor, William Saxbe, said he authorized three warrantless "national security" taps his first week in office—whether against foreign embassies or American citizens he did not make clear.

Senator Nelson's bill would close this final loophole by requiring the Government to go into Federal court and get a judicial warrant for every wiretap it wanted to install. If a tap were to be requested on the phone of an American citizen, the Government would have to show "probable cause" that a crime was about to be committed; if the request was for a tap on, say, a foreign embassy, only a national security reason would have to be adduced. And any American citizen tapped after issuance of a court order would have to be informed of the tap within thirty days, unless the Government obtained a court-ordered delay.

There is no reason to suppose that judges would not issue wiretapping warrants when justified, or that they would thereafter disclose national security information that might have been presented to them. But there is every reason to believe that the Nelson bill would give needed contemporary meaning to the Fourth Amendment's guarantee of "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures. . . ."

[From the Washington Post, Mar. 21, 1974]

(By Gaylord Nelson)

'NATIONAL SECURITY' TAPS

Civil rights leader Martin Luther King, Jr., newspaper columnist Joseph Kraft, former Nixon presidential aides William Safire and John Sears, former National Security Council staff members Morton Halperin and Anthony Lake, former congressional aide Dunn Gifford, and boxer Muhammed Ali—these citizens have something in common. Their telephone conversations have been wiretapped by the federal government for so-called "national security" reasons. And they are merely a handful among thousands.

In each case the government acted without obtaining a judicial warrant approving of the "tap." The government therefore did not explain to a court the justification for the surveillances. Nor did the government voluntarily inform any of the individuals involved that their telephone conversations had been secretly intercepted. Most of those tapped never learn about it.

Despite the righteous indignation of congressional representatives, lawyers, and the public, warrantless wiretapping continues. Last January the Justice Department reported that in one week it had authorized three warrantless wiretaps in national security cases—an average week's quota according to the department. The department did not indicate whether the taps included surveillances of American citizens. Nor did the department indicate the basis for believing the taps necessary. And that is precisely the problem.

Warrantless wiretaps give the government an unreviewed and unchecked power to invade a citizen's privacy. The government alone determines whom it should tap and when it should tap. Neither a court, nor the Congress, nor the individual involved has an opportunity to demonstrate that there is no justification for the tap.

Because they escape scrutiny by anyone outside government, warrantless wiretaps are a dangerous and fundamental assault on the individual's right to privacy and other civil liberties. They pose a threat to the freedom of every citizen, regardless of his or her station in life. In a 1928 surveillance case Supreme Court Justice Oliver Wendell Holmes called warrantless wiretaps "dirty business." In 1931, J. Edgar Hoover—who by then had been FBI director for seven years—called them "unethical" (his position softened in later years).

Warrantless taps also are, in my view, unconstitutional. The Fourth Amendment explicitly provides that every citizen should be free from government searches and seizures that are not authorized by a judicial warrant. There is no exception for "national security" cases. The basic notion underlying the

Amendment is that a neutral court—not a government blinded by its lawful investigatory responsibilities—should decide whether any search contemplated by the government is reasonable.

In the 1967 *Katz* and *Berger* decisions, the Supreme Court held that the Fourth Amendment's protections apply to government wireapping. The Court also held in the 1972 *Keith case* that the government could not wiretap American citizens without a judicial warrant even when the citizen's activities threaten "domestic security." The Court reserved judgment, however, for those cases in which American citizens have a "significant connection" with foreign powers and their agents.

Because the Court has not yet decided this latter question, the present administration maintains that the government can, without a warrant, tap American citizens and others whose activities involve foreign affairs. It was on this basis that the Justice Department authorized three warrantless wiretaps last January.

Congress should not tolerate the continued use of these warrantless wiretaps for so-called "national security" purposes. It is indeed ironic for the government to invoke "national security" to violate those constitutional rights and liberties which the government is obligated to defend. Any remedial legislation should include at least four basic elements.

First, before the government could wiretap American citizens for national security purposes, it should have to obtain a judicial warrant based on probable cause that a crime had been or was about to be committed. This provision would simply recognize the rights guaranteed to every citizen by the Fourth Amendment.

Second, before the government could wiretap foreign powers (i.e., embassies) or their agents, it should have to obtain a judicial warrant based on a belief that the surveillance is necessary to protect national security. The warrant standards for foreign power taps should thus be less rigorous than those applied to American citizens.

The justification for this second provision is plain. The government's desire to wiretap should be reviewed by a court. There should be no exceptions. Otherwise the exceptions could be stretched to sanction an unreasonable invasion of an American citizen's privacy. This second warrant requirement would in no way undermine the government's ability to protect against foreign attack or subversion; the government would be able to wiretap foreign powers and their agents any time there is a real need.

Third, every American citizen wiretapped should be informed of the surveillance within 30 days after the last authorized interception. This would afford the individual an opportunity to protect against violations of his constitutional rights. The disclosure of the wiretap should be postponed, however, if the government satisfies the court that the person wiretapped is engaged in a continuing criminal enterprise or that disclosure would endanger national security interests.

Fourth, there should be continuing congressional oversight of wiretaps and other surveillance activities engaged in by the government. At least once a year, representatives of the government should testify, under oath, before a joint congressional committee about their surveillance activities. In this way, Congress can determine whether the government is complying fully with the laws and whether additional legislation is needed to protect individual privacy.

A number of Senators have joined me in introducing two bills (S. 2820 and S. 2738) which incorporate these basic elements. Other bills might be able to improve on these measures. But in any event, the need for congressional action is clear. A citizen's constitutional right to privacy should not exist at the sufferance of some government official's definition of "national security."

Mr. KASTENMEIER. The Chair would like to observe, while he is not a witness, the presence of General Kenneth Hodson who is Executive Director of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, which is about to undertake its work. Both Congresssman Railsback and I serve on the Commission and we wish General Hobson the best on his undertaking.

I would like to call on my colleague, from Maryland, Congressman Clarence Long. Congressman Long is the author of legislation which would make illegal the practice of secret electronic monitoring and recording of conversations, under certain conditions.

I am pleased to greet my friend and colleague, Congressman Clarence Long.

TESTIMONY OF HON. CLARENCE LONG, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MARYLAND

Mr. LONG. Thank you, Mr. Chairman. I am very pleased to have this opportunity to speak to the distinguished subcommittee about the need to protect the right of an American citizen to have his personal and private communications remain private.

The disclosure last summer of the White House practice of recording the conversations of important officials of the Government, diplomats, and even White House staff members—secretly and without their knowledge—shocked the entire Nation. The White House bugging, however, is only the tip of the iceberg. Throughout the country, persons who have assumed that their private conversations were private have been rudely awakened by the widespread incidence of uncontrolled eavesdropping.

My bill, H.R. 9667, would amend title 18, section 2511 of the States Code to require the consent of all parties to a conversation before it may be recorded or otherwise intercepted.

It is important to emphasize "all parties." If there are a half-dozen people in the conversation, they must all be notified that whatever they say is being electronically recorded. As the law now stands, if only one of the parties knows, there would be no violation.

My bill would make such bugging punishable by fines ranging from $10,000 and up to 5 years in jail, and violators would also be subject to civil suits. The courts would, of course, retain the power to authorize wiretaps for investigations involving criminal activities, or national security.

I think there was a very useful colloquy between the gentleman from Massachusetts and Senator Nelson on the question of National Security wiretaps. I want to leave that area open.

All I am saying is that, under my bill, a conversation could be recorded by the police under a court warrant pursuant to a criminal investigation.

Now, as Mr. Drinan has pointed out, the courts may unduly issue warrants. But I don't think a court would have ever issued a warrant to allow the President to tape the conversations of the people with whom he was conversing. There are many other instances in which courts are unwilling to issue warrants. Therefore, I think my bill would be very useful.

Twenty-five of my colleagues have joined me in sponsoring this measure.

I want to point out that my home State of Maryland has, since 1956, had an official policy of protecting private communications which could well serve as a model for the Nation.

The Maryland statute provides:

> The interception and divulgence of a private communication by any person not a party thereto is contrary to the public policy of this State, and shall not be permitted except by court order in unusual circumstances to protect the people. It is further declared to be the public policy of this State that the detection of the guilty does not justify investigative methods which infringe upon the liberties of the innocent.

U.S. District Court Judge Gesell recently pointed out that legally sanctioned snooping has become a common practice which has been able, under the present Federal law, to proliferate without judicial supervision.

I would like to put in the record an excerpt here from Judge Gesell's statement.

Mr. KASTENMEIER. Without objection, that excerpt will be received and made a part of the record.

[The statement of Judge Gesell follows:]

> Informers, in return for government promises or hope of favors, are equipped with recording devices and sent into the homes and offices of their friends and confidants to try to trap their words on tape * * *. Many individuals, without any knowledge of the government, secretly tape their own conversations with others for ulterior purposes and use casual remarks to extort or intimidate * * * 366 F. Supp. 994.

Mr. LONG. The time has come to protect individual citizens against unrestricted wiretapping, spying and surveillance.

I might point out that we all talk informally in ways that are very different from the way we would talk if we knew that the world were listening. So this legislation is important not merely in cases where life or liberty is involved, but in other cases as well.

A recent Harris poll confirms the timeliness of such legislation. By 77 to 14 percent the public favors passage of a law forbidding such intrusions into their private lives. The Watergate affair may have acted as a trigger to public opinion, as Mr. Harris pointed out, but there has been a widespread and underlying shift towards greater protection of the constitutional right to privacy.

The President himself has now recognized the need for a new law. In his State of the Union message, the President told the Congress that we need "a new set of standards that respect the legitimate needs of society, but that also recognize personal privacy as a cardinal principle of American liberty."

It is my hope that this subcommittee will report favorably on this legislation, which deals with one aspect of the privacy issue which you are considering in a much wider context. Thank you.

Mr. KASTENMEIER. Thank you very much. You have touched on an area which is certainly part of the general problem. I take it that you would contemplate wiretapping in only two situations: One in which wiretapping is authorized by warrant through the courts, and the other is the situation in which all parties consent?

Mr. LONG. That is right.

Mr. KASTENMEIER. Consent in advance to the recording of the conversations?

Mr. LONG. Yes.

Mr. KASTENMEIER. Do you have reason to believe that you yourself may have been a victim of eavesdropping?

Mr. LONG. No, I have no reason to believe that. I never felt I was important enough for anybody to do this to me.

Mr. KASTENMEIER. You know there are Members of the Congress as well as many other people who feel and presumably have knowledge of the fact, that they have been the subject of such types of wiretapping or electronic eavesdropping. The argument is made that some people or entities desire to record conversations to protect themselves by having an exact account of the conversation. But it is your view that any such reason is outweighed by the fact that another person did not know of the conversation being recorded. And that that person's rights outweigh the desire of the person who is recording the conversation for purposes of some form of protection or official account?

Mr. LONG. I am not quite certain that I understand the gist of your question.

Mr. KASTENMEIER. I am asking whether you can contemplate any good reason why, other than through a court warrant, a person or an entity with his own consent should be able to record a conversation even without the knowledge of another person?

Mr. LONG. I tried hard during the drafting of this bill and I couldn't think of any such reason. It is always possible, I suppose, that you can come up with an exceptional situation. We all know that such cases require a balance of rights and privileges.

I don't think there are any absolute rights or privileges written anywhere in our law. There are always conflicts.

I suppose a person could argue that he could obtain a better historical record of what people are really thinking and saying if they didn't know they were being recorded. If he is writing a book, for example, he may think that if he can get people to speak very frankly, then he would get a much better book than if the people were told in advance that their words were being recorded.

I realize that somebody might think that. I don't think he would be justified in inflicting such recording on unsuspecting people.

Mr. KASTENMEIER. I yield to the gentleman from California, Mr. Danielson.

Mr. DANIELSON. Thank you, Mr. Chairman. Mr. Long, would you tell me please what you mean by the word "intercept" in your bill?

Mr. LONG. Record.

Mr. DANIELSON. You talk about to record or otherwise intercept.

Mr. LONG. In doing this I simply used the language of the bill itself.

Mr. DANIELSON. Yes, I know. I have looked at your bill and I assume that all of these different versions of the bill are the same. But it says "electronically record or otherwise intercept a wire or oral communication" and that appears in the printed bill as well as in your presentation.

Mr. LONG. There is a definition of "intercept" in the bill. I don't have it.

Mr. DANIELSON. I have here, for example, H.R. 9973, which is one of your bills, and starting with subparagraph (c) on line 6 it states: "It shall not be unlawful under this chapter for a person to electronically record or otherwise intercept a wire or oral communication" et cetera.

I was just wondering what you really had in mind by the word "intercept" as used in your bill?

Mr. LONG. As I say, we have taken that language from the present law. I can supply the definition for the record.

It is my understanding this means to record. It is a legal term.

Mr. DANIELSON. That is all you have in your mind, to record?

Mr. LONG. Or otherwise get it on record or eavesdrop.

It is somewhat broader than recording. That is to say, it would include a situation in which people simply listen in on a private conversation, people outside holding their ear up to the wall and listening to the converastion of others with the assistance of some mechanical device.

Mr. KASTENMEIER. If the witness would yield, perhaps the Chair could help in the definitions of "wire interception" and "the interception of oral communication".

The definition, as used in Public Law 90-351, is that "intercept" means, "the acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or any other device."

As used in your bill, I assume it is consistent with that definition?

Mr. LONG. Right.

Mr. DANIELSON. You do not restrict it to a surreptitious type of interception in other words?

You are talking about a situation even where all of the parties may be consenting?

Mr. LONG. If all of the parties are consenting, then it is not unlawful.

Mr. DANIELSON. Except for an unlawful purpose, correct?

Mr. LONG. Except for an unlawful purpose.

Mr. DANIELSON. Suppose you and I had an office, and within our office we had a sensitive microphone which was affixed somehow or another to a recording device so that when people came in to visit with us you and I would know that the conversation was being recorded if we turned on the switch, although those people visiting us would not be aware of that fact. That would be an interception within the meaning of your bill?

Mr. LONG. Right.

Mr. DANIELSON. And it would be the sort of conduct that would be unlawful under your bill unless the other party to the conversation consented in advance?

Mr. LONG. Exactly. And my understanding would be, if all parties had knowledge that what they said was being recorded and intercepted, and they continued to speak, this would be implied consent.

Mr. DANIELSON. Right.

Mr. LONG. I can give you another example which frequently happens with me. A constituent calls me and asks me to do something for him and I immediately put a secretary on the line to write down all of the information: what the persons wants, what he needs done, what relatives he needs to have helped, how old they are, what their background is—details that I can't remember. We tell the person that somebody is on the line.

Mr. DANIELSON. Right.

Mr. LONG. And somebody is listening. But it would be possible, in many cases, not to let him know that this is being taken down. My bill would cover such situation.

Mr. DANIELSON. I was going to lead into that. That is the old practice of advising your client that you are going to put the secretary on the extension to make notes?

Mr. LONG. Right.

Mr. DANIELSON. That situation would be included within your bill?

Mr. LONG. Exactly.

Mr. DANIELSON. And would be either lawful or unlawful depending upon whether or not this consent was obtained?

Mr. LONG. Exactly. And I see no harm in that.

Mr. DANIELSON. I do not myself. Being mindful of the fact that today the state of the art in making recording devices is very far advanced, and it is a simple matter to make a tape of almost any type of a conversation, be it on the telephone or otherwise, I want you to address yourself to the practical aspects of it, though. Almost anyone today for less than $50 can buy a rather effective tape recorder plus a little device that will attach with a suction cup to the telephone and make a relatively good tape recording.

Mr. LONG. I understand the recorders don't always work that well.

Mr. DANIELSON. Of course neither you or I have ever tried it, so we don't really know. But let me ask you this. Do you think as a practical matter that this could very well be enforced? It is just about as common today for people to have a tape recorder as it is to have a radio, for example. They are most common and most widespread.

Mr. LONG. Of course, there are many more laws on the books than it is possible to enforce, and in many cases there would be conversations which nobody would particularly care about one way or the other. But I do think there would be a real deterrent effect upon a person who proposed to use such recordings for some malicious or unlawful or otherwise injurious use.

Mr. DANIELSON. Right.

Mr. LONG. I certainly wouldn't want to do it. I would want to be very careful about obeying the law.

Mr. DANIELSON. I think you are absolutely right. If nothing else, it would make such conversations, since it would be unlawful in the first place, it would make them inadmissible in evidence which would have a deterring effect. I can see value there.

But as a practical matter, I should think it might be difficult to police if you were really trying to go out and police it thoroughly.

Mr. LONG. I think this is true of almost all of our laws. If we could enforce all of our laws, there wouldn't be enough jails to hold all of the criminals.

Mr. DANIELSON. Let me change slightly here.

Suppose after a conversation, in the same situation described in my first example, after the visitor leaves the person with the microphone and the recorder in his office, dictates into the recorder the substance of the conversation as well as he or she remembers it or calls in the secretary and dictates the same thing. Do you see any objection to that sort of recording of the conversation?

Mr. LONG. Are you speaking of a situation in which there had been a conversation involving several people and they all were informed in advance?

Mr. DANIELSON. Even if they have not. Let me recast the situation. You have a conference in your office, you and three other persons. Let's say A, B, and C. And after the conference—and this is an important matter—after the conference they go home and you either call in your secretary or pick up your dictating machine and dictate a memorandum of what was said by whom, and about what. Now you have no objection about that I guess?

Mr. LONG. No, of course not, because the person's own words could not be used against him. He could point out that he was not present when the memorandum was dictated and he could challenge the other party's recollection or understanding of what went on.

Mr. DANIELSON. In other words, he is in a position to deny it?

Mr. LONG. Exactly.

Mr. DANIELSON. But he is not in a position to deny it if it is recorded?

Mr. LONG. No, if it is recorded, all of his words are laid out before him.

Mr. DANIELSON. Right. How do you answer the argument that some people advance of, well, the recording is obviously a far more accurate recasting of what was said. In fact, it isn't a recasting; it is a playback, so therefore, it is far more accurate than any subsequent memorandum ever could be?

Mr. LONG. I think such recordings can be very useful, very valuable. And I see no objection to recording just as long as everybody in the conversation knows what is taking place. Basic fairness justifies such a requirement.

Mr. DANIELSON. I tend to agree with you, but I think what we are talking about is what some people call the sporting theory, in other words, for Heaven's sakes, don't have an advantage over the other guy. I tend to agree with you.

What we are really saying is the more accurate account of the conversation is the recording but we must not use it because it gives the secret recorder an advantage that the other person does not have.

Mr. LONG. My proposal in no way stops any recording. It simply requires notice to all parties that what they say is being taken down or intercepted. Thereafter, whatever they say is a matter of record.

Mr. DANIELSON. I think you have a pretty good point here. Thank you so much.

Mr. LONG. You're very welcome.

Mr. KASTENMEIER. The gentleman from New York, Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman. And thank you for your testimony. I think it is very interesting. I would like to continue along the lines of Congressman Danielson in discussing the difficulty of enforcing your proposal.

He mentioned the fact that a lot of people have recorders today, and I guess there is quite a habit on the part of people to record favorite music that comes over the radio or television. I suppose that the doing of that technically would be covered by your bill

and would be unlawful, and it would of course be almost impossible to police.

Mr. LONG. I might reply to the distinguished gentleman from New York that it certainly would deter the party who had recorded this without the other person's knowledge from ever using it against that other person. As soon as he brought out the fact that these remarks had been recorded and the other person hadn't consented to it, it would be an admission that a crime had been committed.

He would not be able to use the other person's words against him in any kind of legal way.

Mr. SMITH. No, I agree with that. But I would expect that under your bill as written, the mere recording of that without the consent of the originator of the conversation or the music or whatever it is, would be unlawful?

Mr. LONG. It would be unlawful.

Mr. SMITH. It would probably never be caught.

Mr. LONG. There are circumstances in which you might never be able to enforce this law. In other words, a person might make such recordings and in certain situations, it would probably never be caught.

Mr. SMITH. Mr. Chairman, I think we had some talk about this kind of thing when we were considering copyright of sound recordings.

One other question, Dr. Long. I would like to point out that probably this wouldn't cause much trouble. But as we watch football games, for instance, on television they have an electronic sound gatherer at the side of the field and, as they come into the huddle, you can hear the quarterback giving the signals and so forth. I would suspect that unless they got the consent of the quarterback and perhaps any other member of the two teams who might speak, they would technically be in violation under this law?

Now I suppose that wouldn't cause much trouble except to make it a little more inconvenient for the telecasters who might want to listen to the sound as well as look at the view.

Mr. LONG. Yes. That is a valid point. I think, and don't you agree Mr. Smith, that this is one of those commonsense problems involved in any law? There are always areas that are beyond the purview of strict statutory gauge.

Mr. SMITH. Yes, as Mr. Danielson pointed out, it is certainly not your intent to make such activity unlawful.

Mr. DANIELSON. Would the gentleman yield?

Mr. SMITH. I would be happy to yield.

Mr. DANIELSON. I think implicit in the bill is the idea that this is a public statement, and that the people who are playing football down on the field know that the public is watching them and so on, and I think there is an implied consent to that sort of thing. I know I record some of our prominent officials' speeches on television. I oftentimes record them so I can savor the juicy comments when I play them back.

Mr. SMITH. Under this bill you would be technically violating the law.

Mr. DANIELSON. Well, people have called me illegal or something like that before.

Mr. LONG. I think you have made a very valid point. It could be printed on the ticket that admission to the game implies consent of being photographed as part of the televising of the game and so forth. I do think there are ways in which this could be handled.

I point out also that if we had this law at the time that these conversations were taped in the White House, it would have made a great deal of difference in the disposition of the whole Watergate case and it could have been immediately clear that in this situation there was the commission of a serious crime.

Mr. SMITH. That might have protected the President against slanderous claims also.

Mr. LONG. That is also possible.

Mr. KASTENMEIER. The gentleman from Massachusetts.

Mr. DRINAN. Thank you very much. I welcome your interest and involvement in this area, Mr. Long. Don't you actually go beyond the Maryland law? You state here in your testimony that "it could serve as a model for the Nation." And yet the Maryland statutes provide that the interception and divulgence of a private communication is illegal. But as I read your good bill, you say that the mere interception even without divulgence is erroneous. It is illegal?

Mr. LONG. That is right.

Mr. DRINAN. Do you actually go beyond the Maryland statute? So you have a supermodel? I mean, the Maryland statute is defective in your opinion?

Mr. LONG. I would go beyond that because I think that interception of private conservations must be discouraged. That is a very good point.

Mr. DRINAN. I have a constituent who claims that the phone company is listening to him and he has some plausible evidence. Would your bill applv to the phone company?

Mr. LONG. The present law, which would not be affected by my bill, states in title 18, sec. 2511(2)(a)(i):

> (2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights of property of the carrier of such communication: *Provided*, That said communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

Mr. DRINAN. Thank you. That clarifies it. One last point.

I thank you for the reference to my dialogue with Senator Gaylord Nelson. And I was trying to make the point, and maybe I didn't make it very clearly, but the ACLU position is categorically opposed to all wiretapping and has been since May 1961. They have said that the ACLU stands unequivocally against wiretapping or the use of other electronic eavesdropping devices by any person for any reason whatsoever.

You kind of suggest that the need for wiretapping legislation is moot. I hope it is not. I hope it is a live option and maybe the Congress will follow what was recommended by the ACLU 14 years ago.

Mr. LONG. As I said before, I really don't want to get into that.

Mr. DRINAN. I know. Thank you.

Mr. KASTENMEIER. Did you want to comment further on that?

Mr. LONG. No.

Mr. DRINAN. Thank you very much.

Mr. KASTENMEIER. The gentleman from Iowa, Mr. Mezvinsky.

Mr. MEZVINSKY. I want to commend the gentleman from Maryland. I think his contribution is significant, but I really have one question in view of the comments concerning enforcement.

You pointed out that if you really wanted to enforce the laws, you wouldn't have enough jails to put all of the violators in.

Mr. LONG. I think that Shakespeare wrote that if you put everybody who deserves to go to jail in jail, where would there be any honest men to keep them there?

Mr. MEZVINSKY. I guess in view of Shakespeare and in view of your remarks, I want to know, how do we hope to enforce this law?

Mr. LONG. Civil suits would be a self-enforcing aspect. If any person felt that his conversations had been recorded, he could bring this out as part of a civil suit or part of a complaint. That would be one way of handling it. Another would be that the person who had acquired this recording as a scheme against another person would be precluded from using it in any legal way because he had committed a crime in acquiring the recordings. That would be a very important self-enforcing aspect.

Mr. MEZVINSKY. Thank you very much.

Mr. KASTENMEIER. The committee is grateful to you Congressman Long for your testimony this morning and for the bill you have introduced, which is one of the issues we will have to confront.

Mr. LONG. Thank you, Mr. Chairman, and the committee for hearing me. I certainly enjoyed the presentation.

[Mr. Long's statement follows:]

STATEMENT OF HON. CLARENCE D. LONG, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MARYLAND

Mr. Chairman, I am pleased to have this opportunity to speak to the distinguished Subcommittee about the need to protect the right of an American citizen to have his personal and private communications remain private.

My home state of Maryland, since 1956, has had an official policy of protecting private communications which could well serve as a model for the nation. The Maryland statutes provide that:

"The interception and divulgence of a private communication by any person not a party thereto is contrary to the public policy of this State, and shall not be permitted except by court order in unusual circumstances to protect the people. It is further declared to be the public policy of this State that the detection of the guilty does not justify investigative methods which infringe upon the liberties of the innocent. (Annotated Code of Maryland, Art. 35, Sec. 92)."

The disclosure last summer of the White House practice of recording the conversations of important officials of the Government, diplomats, and even White House staff members—secretly and without their knowledge—shocked the entire nation. The White House bugging, however, is only the tip of the

iceberg. Throughout the country, persons who have assumed that their private conversations were private have been rudely awakened by the widespread incidence of uncontrolled eavesdropping.

My bill, H.R. 9667, would amend Title 18, Section 2511 of the United States Code to require the consent of ALL parties to a conversation before it may be recorded or otherwise intercepted. As the law now stands, if "A" and "B" are conversing, "A" could secretly record the conversation without "B's" knowledge—without breaking any law.

My bill would make such bugging punishable by fines ranging up to $10,000 and up to five years in jail, and violators would also be subject to civil suits. The courts would, of course, retain the power to authorize wiretaps for investigations involving criminal activities or national security.

Twenty-five of my colleagues in the House have joined me in sponsoring this measure.

U.S. District Court Judge Gerhard Gesell recently pointed out that legally-sanctioned snooping has become a common practice which has been able, under the present Federal law, to proliferate without judicial supervision. According to Judge Gesell:

"Informers, in return for government promises or hope of favors, are equipped with recording devices and sent into the homes and offices of their friends and confidants to try to trap their words on tape * * * Many individuals, without any knowledge of the government, secretly tape their own conversations with others for ulterior purposes and use casual remarks to extort or intimidate * * *"

The time has come to protect individual citizens against unrestricted wiretapping, spying, and surveillance. A recent Harris Poll confirms the timeliness of such legislation; by 77 percent to 14 percent, the public favors passage of a law forbidding such intrusions into their private lives. As Harris pointed out, while the Watergate affair may have acted as a trigger to public opinion, there has been a clear and underlying shift toward greater protection of the constitutional right to privacy.

The President himself has now recognized the need for a new law. In his State of the Union message, the President told the Congress that we need "a new set of standards that respect the legitimate needs of society, but that also recognize personal privacy as a cardinal principle of American liberty."

It is my urgent hope that this Subcommittee will report favorably on the legislation which I and several other Members of Congress have proposed in order to safeguard the personal nature of a citizen's private communications.

Thank you, Mr. Chairman.

Mr. KASTENMEIER. The Chair would like to greet as our next witness Mr. William Turner of California.

Mr. Turner has served for over 10 years as a special agent with the FBI. Since he resigned from the Bureau in the early 1960's, Mr. Turner has worked as a private investigator and a magazine editor. He is the author of several books, including "How To Avoid Electronic Eavesdropping and Privacy Invasion."

Mr. Turner would you please come forward. I would say to my colleagues, we do have four witnesses yet this morning and I hope we can proceed expeditiously.

TESTIMONY OF WILLIAM TURNER, FORMER FBI AGENT, PRIVATE INVESTIGATOR, AND AUTHOR OF SEVERAL BOOKS, INCLUDING "HOW TO AVOID ELECTRONIC EAVESDROPPING AND PRIVACY INVASION"

Mr. TURNER. Thank you, Mr. Chairman and members of the subcommittee.

I will try and be as brief as I can. I understand that the purpose in my being here this morning is more or less to get an exposition

or a feeling for what really goes on from the standpoint of some body who engages in the black arts.

I have been on both side of the fence in the FBI. I was a sound man, which is a euphemism for a graduate of the FBI school which teaches bugging and tapping and burglary, and I also have been involved as a writer in the last 10 years on controversial subjects and hence have been on the other side of the surveillance.

So getting into the issue of electronic surveillance, perhaps if I give some firsthand accounts, it would better establish just what we are trying to reckon with in terms of the subcommittee's investigation.

I went into the FBI in 1951. And in 1952 and 1953 I was assigned to the San Francisco office and, because I was a bachelor, I was assigned to the monitoring plants. These were odd shifts. They were manned 24 hours a day. We had one of the plants down in the produce section and we had another one over in Oakland, which carried the recording equipment for all of the installations in the east bay of the San Francisco area.

Since that particular time, while they have had some mishaps, and the FBI monitoring plants are now located inside the field offices. I said "installations" because I am not distinguishing between wiretaps and microphone installations.

In those particular plants and in the current FBI plants, the lines that feed in carry both microphone and wiretap conversations. The plants are for the purpose of monitoring permanent installations. In most cases, what will happen is that the FBI will lease a line from the telephone company, much as radio stations would lease lines, and the line will feed from the particular monitoring point out to where the installation is. And as you can see, there is a considerable amount of logistics involved in this.

In April of 1958, perhaps because of my engineering background, I was selected to attend the sound school of the FBI in Washington. Now these particular schools are held on an irregular basis as the needs to replenish sound men in the field come up. And I should point out that the Treasury Department and the CIA and the various military intelligence agencies do, or at least did, conduct similar schools in the Greater Washington area.

In that particular school, which lasted 3 weeks, there was very little discussion on the part of the instructors on the constitutional issue of bugging and wiretapping. We simply were told that the FBI tapped under two justifications. And here we are getting into a little bit of the evolution of bugging and tapping and the law or the lack of the law at the time.

The two justifications were that President Roosevelt gave executive authority during the war emergency, and that no succeeding President had rescinded that authority; and the second justification was that the element of disclosure in the Communications Act of 1934 was not violated because information obtained was not disclosed outside of the Justice Department.

In other words, they were viewing the Justice Department as a metaphysical entity. The instructor added that the Communications

Act of 1934 was intended not for the FBI, but for telephone employees in league with private investigators.

Now we get into another area here, which is the difference between telephone-connected devices and those which have no connection to the telephone systems at all. In that particular class we were told that the authority for any device connected to a telephone must come from the Attorney General, but that the Bureau installed microphone surveillances strictly on its own authority. So I think that during that period a very misleading picture was portrayed to the Congress and to the public at large in terms of the total electronic surveillance, at least by the FBI.

The announced wiretaps, if I recall, always hovered in the field of 100 nationwide, but that was only part of the picture.

One reason was of course that there were a lot of microphone installations that the Bureau installed on its own authority.

I can cite an example of how these books were kept in order. In one instance I was instructed to put in a wiretap and this wiretap was made. It was very simply made by making a bridge on the pole box not too far from the subject's home. There was no necessity to trespass at all except on the telephone privacy. So that tap was in operation for a couple of years. And it was not furnishing information or intelligence on a continuing basis. It was for a one-shot piece of information.

So I got a letter from the FBI laboratory instructing me to yank that particular tap and in place of it to install a microphone installation. Now this presented an entirely different problem. In order to install the microphone, I first had to have the FBI laboratory fabricate a special device, a small microphone with the little preamplifier inside a connecting block, a regular Western Electric connecting block. I then had to get up what we call a "black bag job" team, which was a burglary team actually, and we had to go through the whole drill of breaking and entering a premises in order to install that particular device, replacing the other connecting block, running wire underneath in the basement of the house, connecting it with fine wire that was concealed inside the drop wire out to the telephone, and then connecting up with the leased line and making the hookup in the FBI field office.

So, in that particular instance, the book indeed was in balance, but I think the Constitution suffered because of the fact that we had to break and enter in order to make the installation.

Going back to the training sessions, they were conducted over in the old Identification Building and in the southwest area of Washington. There was a practice room where we planted bugs in the walls and taps on a mute phone there. We went down to the FBI radio station, which is out in rural Virginia, and practiced pole climbing with regular telephone pole climbing equipment.

In an attic of the Justice Building there was a workshop where the FBI's top burglar taught us how to make lockpicking devices, and how to use them.

And after that course we were sent back out into the field to employ these skills, which I did in the Seattle office, in the Oklahoma City office also, for approximately 3½ or 4 years.

The additional duties of sound men, in addition to these kinds of positive installations, is also the very legitimate function of handling security of the FBI office communications. I can recall that there were tapes made on people involved in the Coors kidnaping of people who were somehow identified with the suspect; there were taps on Communist Party functionaries; taps on various so-called security subjects.

As I said, the permanent installations involved the leasing of a line from the telephone company under some cover name such as the Federal Research Bureau.

Down in Las Vegas, the FBI used the Henderson Novelty Co. I suspect that the telephone company knew all along the purpose of our request for a line that was not ordered hooked up at either end. And the way that we went about getting those kinds of lines, or any kind of special consideration, such as the hookup of the recorder in the telephone company central office, was to maintain a liaison with the special agents of the telephone company. In some instances, they were former FBI agents. In most instances, they were former law enforcement officers. And they would assist with these arrangements. They would furnish information from the subscriber's cable card, that was necessary to install the tap, and they would notify us if telephone company personnel found a tap or a bug that we may have put in.

I can recall being called by a special agent of the telephone company and he asked me about a little thin wire hanging down from a telephone pole. I thought I got it in the cracks pretty well, but a telephone lineman on a service call found it.

He called me immediately and asked me if I knew anything about it. I said I did and that was the end of it.

This particular installation I made in terms of what we call a "suicide tap". A suicide tap was one that was installed strictly on the initiative of the agents in the field and of course in collaboration with the sound man. It was called a "suicide tap" because it was strictly unauthorized by Washington and usually was authorized by the agent in charge of the field office. And it does illustrate the problem of training and equipping people with the necessary skills and knowledge and equipment to go out and use this kind of a black art and still try to control it, either from Washington or through some kind of central authority.

I mentioned the burglaries. The FBI alluded to the burglaries as "black bag jobs" after the kind of doctor's kit that the tools were carried along in. And when I entered the Bureau in 1951, black bag jobs were spoken of in terms of being a standard technique, just as tapping phones and mail covers and trash covers. They were conducted for two main purposes, the first was, as I have recounted one episode, to install a microphone inside a premise. And the second purpose was to gather intelligence and to photograph documents.

Now the black bag job is different from a conventional burglary in that nothing is removed and every effort is made to disguise the fact that entry was made.

I participated in a number of black bag jobs, including a 1957 burglary of the Japanese consulate in Seattle. And in that operation, the top burglar flew out from Washington. He used radioactive cobalt to bring out the arrangement of the locking mechanism. And after a period of hours, was able to open the safe. The contents were photographed and returned to their exact position in the safe.

In these kinds of operations, elaborate measures were taken to insure the security of the black bag job participants. In the first place, we were instructed never to take anything that would identify us with the FBI in the event that an unfortunate mishap occurred.

Just like in a bank robbery, the premises were thoroughly cased to make sure that the identity of the regular occupants were known and their normal movements were known. And when the black bag job was about to take place, surveillances were put on them in order to make sure that they didn't double back to the premises.

A further precaution was to station an agent at the police radio conosle to make sure the complaints of a burglary in progress were not answered.

The FBI agents who made a specialty of black bag jobs were frequently rewarded by meritorious cash awards, which of course would not be identified as to their reason.

Now getting into the area of the actual technical surveillances, as it is called, and the FBI referred to it as Tesurs, the FBI refers to wiretaps as Tesurs, which is a contraction of technical surveillance. And it refers to microphone or bug surveillance as Misurs.

There are two kinds of telephone taps: the direct and indirect A tap-transmitter in which a phone line is tapped and the conversation strictly limited to the telephone conversation is sent over the air to a receiving point and is, as I say, the tap-transmitter. The advantage of this to the tapper is the tremendous security because, if the device is found, it is not traceable to him. If the wires lead direct to a monitoring post, why the lines are of course traceable.

An additional element of security is afforded by what the telephone company in its construction practice calls the multiple appearacne. Multiple appearances means that your particular telephone line will appear not only in the pole box nearest to your premise, but will appear in another one perhaps in a radius of a mile simply to allow for the two-party subscriber. And usually that other pair is vacant. If the tapper knows where to go to find it, this involves the cooperation of the telephone company cable records, of course, he can tap at that site in relative security.

Again, getting into the problem of control of wiretaps, a few years ago again when the FBI was contending that there were perhaps 100 taps nationwide, Ronald Kessler did a very thorough investigation for the Washington Post. And in that particular investigation he disclosed that the FBI had 450 special service lines feeding into the Washington field office from all over the city.

Obviously perhaps on a kind of multiple phone, a rotary phone, one tap would involve maybe 10 lines if you are tapping one establishment. But I think that the fact of those very many lines indicates again the need for some kind of outside authority to look into

unilateral statements on the part of agents who engage in electronic surveillance.

The question of microphones and bugs, again they fall into two categories: wired and wireless, which is the bug transmitter or the microphone transmitter

The wired simply means that the microphone is connected to that listening post by a run of wire. For example, the installation in Seattle, where we picked the lock to enter the dwelling, in that installation, the technique that was used there was simply to run a very thin wire concealed behind a baseboard from the microphone down into the celler, run it behind rafters in the celler, drill a hole, and the FBI already had furnished me with a telephone company drop wire that was especially built and that had two very fine wires running through it. And they were connected on. The telpehone drop wire then carried it out to the pole box.

I had one problem after we hooked up that because there was a nearby commercial radio station interfering. Apparently the bug wire was acting somewhat like an antenna so it was simply a simple matter to design a low pass filter and filter out that radio frequency.

The wireless type I think at this stage is the most common. It can be planted strategically, and again if it is discovered, it is not traceable to the eavesdropper. He is simply out the $50 or so a decent one costs.

And the wired type again is very vulnerable to detection because of the necessity for wires to run all of the way from the installation to the monitoring point.

I have in my black bag here [indicating] an illustration of a very modestly priced bug. And since the law at the current stage forbids possession, I should point out that this equipment is all disarmed much like an automatic weapon with the barrel plugged.

This one [indicating] very simply is a small pillbox with a pretty good circuit inside. I should point out that every bug in order to operate with any range at all requires an antenna. So again the element of looking for a particular bug would involve, if you suspect one, that there has got to be an antenna somewhere, which adds to the bug's insecurity.

This one [indicating] is just a little 9-volt-battery type with a 9-volt battery that hooks in there. And the way it operates, as you can see, if you found this, it wouldn't be much loss to the tapper.

It can be received simply in a radio this small [indicating], which is an ordinary transistor radio. It is an FM radio. The upper band here [indicating], well the whole band has been slid down a little and the commercial ends right about here [indicating] and then here [indicating] is your bug band, right here [indicating], right at the top.

And this kind [indicating] of a bug is very difficult to trace. These are just standard components that any kid perhaps with a high school electronics shop experience could put together.

Here is one [indicating] that is a little more mass-manufactured. This is an FM wireless microphone. And again, it is the same situation. This one would cost in the neighborhood of $70 and a couple of little 9-volt batteries.

Mr. KASTENMEIER. And the way that operates is that that is placed or situated in, for example, a room and it is live 24 hours a day?

Mr. TURNER. Yes.

Mr. KASTENMEIER. And it transmits all sounds?

Mr. TURNER. Yes.

Mr. KASTENMEIER. All sounds in the room?

Mr. TURNER. Exactly, Mr. Chairman.

The bugs again, as you point out, carry all conversations; pillow talk as well as relevant conversations. And I would place them in a little more insidious category for that reason.

One of the problems of course, is that your batteries will run down. Again, whenever you hide something like this, you have to have some air conduction in order to get a good pickup. So there are technical problems confronting the bugger.

Nonetheless, if I had some room and could install a number of batteries in parallel, if the bugger could do that, he would get very long battery life and this could go on for some time.

There is also the advanced bugger who has a remote switching device where he can turn it on and off simply when he wants to monitor, again conserving battery life. Otherwise, he would have to reenter and replace the batteries.

The other thing that he may do is, if he want to plant a very small device in a wall with say a very limited range, he may have a repeater somewhere nearby; a kind of booster station that will boost his signal along. Then if he is monitoring in a car somewhere, you have the same problem of enforcement that you would have in the case of say narcotics where you have to catch somebody with the narcotics. In other words, how do you catch this man with the bug. He is not connected to it in any other way except the airwaves. And it is a very difficult problem of enforcement.

I have another device here and I think this is very illustrative of what the 1968 law meant. In fact I think the legislative history brings this out. I have a device primarily useful for aural acquisition. It is called a spike-mike and it is employed usually from the room next door or from some outside area. Here it is [indicating].

It simply is a contact microphone. It is a crystal microphone of very good fidelity. And the tapper then takes one of the spikes and screws it in here [indicating]. Well, actually first he puts this into the wall and this makes contact with the inner wall. This [indicating] will go through. I have another size here if it is a thinner wall.

And that mike as I say is very sensitive. It then is plugged into an amplifier. And he can either feed into a recorder or he can listen with his earset. And this as I say is an example of something that I can hardly conceive of being used as a baby-sitter device or something for party fun or the other kinds of reasons that are now given for making these kinds of devices that are not primarily useful. They may have double or triple purposes.

Then you have the stethescopelike device, which you can affix to a wall. These are usually very transient types of installations.

Somebody checks into a motel room for instance, this is the ideal kind of piece of equipment to use in that situation. It is not like

the permanent leased line situation, which is for a long-term intelligence gathering.

There has been much made lately about the state of the technology. And indeed the technology, aided and abetted by space-age developments and all, has gone on and gone forward.

I think another committee in the past looking into this problem was regaled with the olive-in-the-martini type transmitter. And while such a device exists, I think it is highly impractical and not one of the main problems confronting legislatures in this area for the simple reason that the thing is so impractical. It will hardly transmit more than a few feet. You know, you have to be a few stools down to pick anything up.

And there is talk about the CIA having perfected a laser device that aimed at a room window will pick up the room conservations from the minute vibrations of the glass pane. I am sure if that isn't in a perfected stage, it is very close to it.

But again you are getting to the problem that this type of device would be available simply to the agency that would perfect it and so it would take immense amounts of money needed to purchase one.

Tiny integrated circuits have been developed for the aerospace programs and these obviously don't bode well for future privacy as they are the breadboard upon which a bug can be made.

There is also a device called the infinity transmitter, or harmonica bug. And for example if I went into an apartment in Honolulu—well, let's use another example. I am not sure whether we have direct dial to Honolulu.

In Los Angeles, if I installed a little device in a telephone and I came back to Washington, if I had this infinity transmitter, I would simply direct dial that phone, and then, as soon as the line clicked on, I would activate this device which would then freeze the ringing system on that phone and it would at the same time activate the bug in the phone so that in Washington, D.C., via the telephone longdistance line, I would be monitoring the room conversations in that apartment in Los Angeles.

This state of the art is available to the bootleg eavesdropper. That particular device was marketed in the past before the 1968 law. And since it has now been disseminated throughout the eavesdropping underworld, I am sure that anybody who wanted to pay the price could lay their hands on it.

Next, prevention and detection. It is getting to an area here where again we have problems. If a telephone subscriber suspects a tap, he can request the telephone company to conduct an inspection, but, if the device is found, the telephone company merely turns it over to the proper law enforcement authority. It generally will not advise the customer that he has been invaded.

I think this is an area for legislation, because I don't know that in the 1968 law that under the civil recovery provisions, I don't know whether the plaintiff in a civil suit, the plaintiff having been injured in this fashion, has the availability of the law enforcement testimony and of the law enforcement evidence if a criminal case has not been brought.

And I think that is one area that might be considered in future legislation.

Most law enforcement taps that are conducted under court authority are in the telephone company's central office, which makes detection by the citizens or a private sweeping outfit on his behalf very difficult if not impossible to locate. And contrary to the mythology, a properly installed telephone tap will not cause clicks and noises.

I have gone to the trouble of trying to outline a number of preliminary checks that a citizen can make for devices in the book that I wrote on this.

He can check his premises for such things as fresh plaster marks and alien wires, check for antenna wires of a bug transmitter.

He can hire at considerable cost a professional sweeper, but he should be aware of someone who advertises their services and shows up with simply a kind of wand they call a hound dog or field strength meter, and then declares the premises "clean". Some unscrupulous operators in this field have even planted their own bugs, and then discovered them. This is a prelude for their sales pitch for their periodic services.

A truly professional search requires anywhere from $8,000 to $10,000 worth of equipment and somebody that knows how to use that equipment, who should have gone to the manufacturers' school.

And it should also be noted that bugs that can be remotely turned on and off are very difficult to detect. And, the eavesdropper may plant a decoy bug that is easily found, to lull the victim into a sense of security.

Also the private citizens should beware of delivery men bearing gifts which may contain a bug. And repairmen and utility men who want to enter the premises uncalled for and the salesmen who drop by and leave a briefcase in the conference room and this kind of thing.

There was another area that was brought up and that is the area of voluntary conversations being surreptitiously recorded. And I draw a distinction between interception and that type of voluntary conversation. In other words, if I am talking to a second party face-to-face and the conversation is recorded surreptitiously, by me, I don't find that too much different than if I were taking notes or mentally recording it and later dictating it except of course, as has been brought up already, in the area of again the recording can be used as evidence against him. It does contain his exact words and his inflections.

But again, looking at it the other way, the fact that it does contain exact words and inflections, I think make a more valuable record of what was actually said and I feel that it is not right to legislate against a person protecting himself by recording a free and voluntary conversation.

And I am not talking about a third person being under the table, because that is an interception electronically as opposed to by notes or by mental retention.

And if I was interviewed by a law enforcement officer, in connection with my either being a material witness or possibly a suspect, I would like to have a recording of just what his questions were and what his remarks to me were. And I don't feel it is right that he should be allowed to wear a recorder and I should not be. And so my feeling is that in that area, that the law should be considered to provide for a private citizen also in that type of conversation, making his own recording.

To sum it up, my overall feeling in the area of electronic surveillance is something like the alcoholic who is reformed and doesn't touch a drop.

I am for abolition. And I think the real reason is I don't find any way to effectively control it once it is legitimitized for the law enforcement in the interests of that vaguely definable "national security" or unilaterally definable "national security", or in the area of crime investigation.

If the legislation is going to be that we allow it for certain instances—and I doubt very much whether those of us who prefer abolition are going to get it—then I found that one suggestion that was brought up this morning of placing various heads of field offices under oath to find out exactly what is going on has a considerable amount of merit.

I might also propose the idea of a Federal kind of, well, I don't like to call it a "truth squad", because that implies dishonesty, but a kind of special squad that knows all about wiretapping, bugging, and would go around and have complete entry to the facilities and th agents of any agency that is permitted to use electronic eavesdropping.

I think this way that we would all be alerted to the fact that, if there was any boootleg eavesdropping, that there was a good chance of discovery, and I think this would cut down on it quite a bit.

Well, I—as I said—I think that the area that you gentlemen have embarked on here is one that does cry out for additional legislation and I am very happy to have been invited before the subcommittee to lend whatever I can to the discussions.

Mr. KASTENMEIER. Thank you, Mr. Turner. I think your testimony will be very useful to the committee.

You have given us a background at least, historically, of some of the uses made of the subject matter of this particular hearing.

We do have a quorum call. Let me ask the members of the committee whether you have questions of Mr. Turner, or whether Mr. Turner can leave?

Mr. MEZVINSKY. May I just ask one question?

Mr. KASTENMEIER. Well, I am trying to determine whether or not—

Mr. MEZVINSKY. Oh, I am sorry.

Mr. KASTENMEIER [continuing]. Whether or not you all have questions.

In view of the quorum call, I want to find out whether we can release Mr. Turner or have him return after lunch.

I guess you had better return.

Mr. TURNER. Fine.

Mr. KASTENMEIER. I think we can continue our colloquy then, and trust that the members of the subcommittee will have questions to ask of you, Mr. Turner.

I apologize for the length of time it took with the first two witnesses. Mr. Leon Friedman and Mr. Shattuck and Mr. Morton Halperin, also have kindly agreed to return after lunch.

Mr. SMITH. Mr. Chairman, there is a Judiciary Committee bill. We have the Police and Fire Benefits Act.

Mr. KASTENMEIER. That will not come up until sometime later. I think the Arms Control and Disarmament Act is up first.

I would like to reconvene the subcommittee, if it is agreeable, at 1:30 so we can proceed as far as we can. I trust we can complete the witnesses today.

If there is no objection, then, the subcommittee will stand in recess until 1:30 at which time we will reconvene in this room.

[Whereupon at 12:30 p.m., the subcommittee recessed to reconvene at 1:30 p.m., this same day.]

AFTERNOON SESSION

Mr. KASTENMEIER. The subcommittee will reconvene on matters relating to privacy, wiretapping and electronic eavesdropping. And the Chair would like to recall Mr. Turner, please.

Mr. Turner, I think your testimony this morning was extremely helpful. I am reassured somewhat that what might have been possible for the Government to do surreptitiously in years past is less possible today, partly because of people like yourself, some of them in the military services as well—and I can remember a case or two in your State—of former military personnel who literally blew the whistle on activities such as you have been describing.

Most of what you had described of your own experience in the Bureau was of course before 1968, and so I suppose much of what you might know in terms of present policy and operation would be a matter of not first-hand experience, but just judgments made from past experience.

For example, one of the things that statistics will not show in terms of wiretap applications is how many suicide missions are there. Isn't that correct? Have you any reason to believe that the same suicide missions are not pursued today that were pursued 15 years ago?

Mr. TURNER. Mr. Chairman, you are quite correct. Anything would be hearsay or an impression from staying in contact to some degree with what is going on both through investigative journalism and inside contacts. And there is no reason to believe that it has been terminated forevermore though.

I believe sometimes when the heat is on, especially by subcommittees such as yours, the agencies will pull in their horns quite a bit but I think the history of the thing has been that it has gone back to the status quo or situation normal and one of the problems that I see is in the justifications for say, criminal wiretaps or microphone installations. I find in my own experience that the justifica-

tions offered invariably are ones with which we all would agree. For example, the legislative history of the 1968 act specifically points at a drive against organized crime. And of course I have long written about the dangers, about the corruptive dangers of organized crime and its menace to society as a whole as opposed to some criminals who, heinous as the crimes may be, victimize only one or two people. However, I think that in accepting this kind of justification, that we have to be very cautious as to the possibility that it might be altered at a later date.

For example, in the middle 1950's the Los Angeles Police Department Intelligence Unit, along with similar units from other departments, other major departments across the country, formed what they called The Law Enforcement Intelligence Union, LEIU. The stated purpose of this was to organize a drive against organized crime, recognizing that it was national in scope rather than just a problem confined to Los Angeles, Philadelphia, Detroit, whatever.

They did get up quite a mechanism there in which exchange of information and surveillances, and I suspect they used electronic surveillances, a whole program was instituted. In the mid-1960's, after this apparatus had been set up and was functioning, then Chief Tom Reddin of the Los Angeles department in the course of a press conference, stated that the main danger to the United States was domestic turmoil, and that that particular law enforcement intelligence union had switched targets therefore; it had turned from organized crime and decided that the complete danger to the United States was the radical left, was civil disorder.

So there was a well-intentioned program I think getting a little out of hand there, away from the original intent.

Mr. KASTENMEIER. Yes, sir. I agree. I would like to talk for a moment about the technical aspects of wiretapping. You draw certain distinctions. For example, there are phone interceptions, and there are nonphone interceptions.

Mr. TURNER. Telephone?

Mr. KASTENMEIER. Telephone.

Mr. TURNER. Yes.

Mr. KASTENMEIER. I take it you also referred to other categories such as wired interceptions and wireless interceptions?

Mr. TURNER. True.

Mr. KASTENMEIER. In terms just of the techonolgy, is there some sort of distinction of other catgeories that clearly are identifiable? For example, there is the old-fashioned telephone tap?

Mr. TURNER. Yes.

Mr. KASTENMEIER. There are I assume some of the new subtler devices that trigger the phones automatically from other cities and so forth?

Mr. TURNER. Yes.

Mr. KASTENMEIER. But basically still using the phone, and the telephone line as the means of interceptions?

Mr. TURNER. True. The old bread and butter tap is simply going to say an apartment house, and in the frame, in the basement, finding the subscriber's lugs and just put "alligator clips" across them

with a little condenser, and then you have a pair of earphones and listen in or attach a recorder.

Now there are many variations on that theme of you intercepting that telephone conversation. There is what they call a "hot mike" which is simply in FBI terminology, a "mike-tel", the microphone telephone in other words.

The telephone instrument itself is altered so that when the instrument is in the cradle, the off switch is by-passed and the microphone in the telephone itself is activated and therefore it picks up all conversation, all room conversation and not just the telephone conversation.

I think the recorder you are referring to is what is called VOR, the voice operated relay. When the telephone is not in service, why the recorder is not on. When the telephone is used and there is a sustained voice level on it, the relay switch is on the recorder and that of course conserves tape.

Mr. KASTENMEIER. So that is automatic and does not require manning, require monitoring by one or more individual?

Mr. TURNER. This is true. Again, it offers a certain security in that the person himself does not have to be present while the monitoring is going on.

Mr. KASTENMEIER. You refer to the fact that the Bureau had conducted in Washington a sound school and that some of the other units of government had similar schools. You referred to a sound school. I take it however, that the Bureau and other units of the Government may use devices other than those monitoring sound? For example, do they use cameras and other methods? Is that part of your training?

Mr. TURNER. Well, the training was in electronics and electronic eavesdropping. What Jim McCord would call training to be a wireman, as he calls it, and NYPD calls it a "wireman". In the art there are all different terms.

And that program was for 3 weeks at school. The last 3 days were devoted to lock picking and bypass, as they call it, in order to enter premises, in order to plant electronic devices, but the whole school was taken up with the theory and practice of electronic eavesdropping.

Mr. KASTENMEIER. Was the lock picking aspect justified on any legal grounds during the course of your training or otherwise?

Mr. TURNER. No, there was absolutely no mention of it in terms of any possible infringement of the constitutional rights. I remember at that time I was stationed in the Seattle office and the instructor, when I was leaving, made some crack to me about "well, burglary will get you 8 years in the State of Washington". So there was a rather cavalier attitude toward the whole thing.

I think the attitude in the Bureau then, and perhaps you can try to verify what it is at present, I think the attitude then was pretty much an attitude that the FBI knows best, that we stand between crime and subversion, and if Mr. Hoover says it should be that way, it should be that way. It was a very monolithic organization and the personnel were selected and trained with that type of compliance in mind.

So I believe that the attitude as reflected in that remark and the Communications Act of 1934 was really intended for telephone personnel and not for the FBI. In other words, the laws were really not broken by the FBI, because the FBI was some kind of superseding authority.

Mr. KASTENMEIER. In your own experience and as a matter of your own judgment, I take it that the telephone company was almost without exception cooperative and would cooperate with the Bureau or with the law enforcement authorities, irrespective of the rights of the individual, at least while you were in the Bureau?

Mr. TURNER. Yes, the telephone companies around the United States operate fairly autonomously, and from my own first-hand experience and from talking to other trained sound men when we got together, most of the telephone companies were fully cooperative with the FBI in these endeavors. They put it on the level of it was a patriotic gesture. I don't think that they knew that we had some men that were doing this in criminal cases, even though at that time it wasn't authorized for criminal cases, I mean, we were only supposed to be doing it under national security.

Still, they have one, I remember they had one on Mickey Cohen and some other hoods, about 1958 and 1959, after the Appalachian Conference in 1957, which caused quite a bit of embarrassment to law enforcement as a whole, and many short-cut methods were devised to try to catch up in the intelligence end of it on organized crime.

The New York Telephone Co. is one that I understand they did have a little trouble with. It wasn't fully cooperative. The Chesapeake and Potomac, and I know Pacific was and Southwestern Bell was definitely.

Mr. KASTENMEIER. In terms of private or nongovernmental electronic surveillance, what is your judgment today as to how pervasive or widespread such practices are?

Mr. TURNER. It is a difficult judgment to make, simply because it is not a subject that even private detectives will talk about among themselves. You hear opinions both ways. I think that after 1968, after the act, my feeling is there was a definite curtailment to see which way things would go in terms of enforcement. I think they realize now, and I think it is obvious now, that the enforcement is very difficult. And if you have a throw-away transmitter that nobody can trace, that is made out of parts that are obtainable in any electronics shop and doesn't have a serial number, and maybe somebody finds it and it can't be traced to you, that there really is no risk. But I think that people who want to have that kind of work done by a private investigator can, after making several phone calls, find somebody that for a price will do it.

Mr. KASTENMEIER. What is your experience as to enforcement by law enforcement authorities, either the Federal Government or any other agency of government, as far as curtailing illegal and nonauthorized wiretapping or electronic surveillance? Are there cases that you know of or are there areas where unauthorized tapping is pursued in terms of prosecution?

Mr. TURNER. Well, as far as I know, and I haven't gotten into it with depth, you know, probed the depths of Justice Department sta-

tistics, but they only have had a few prosecutions under this act. One was Gordon Novel, in *United States* v. *Novel*, in Nevada, and if I am not mistaken that case involved, well the count on which he was indicted was bringing a recording device interstate. And they didn't indict him on the use of it, even though it supposedly was planted under a tribal council meeting in order to find out what their feeling was toward the land developers' offer. So there it was not really a direct prosecution under the act itself.

There is the case down in Dallas of the Hunt family. I understand that in that one the motion to suppress has been upheld. And on that case, and I am not familiar with the details on it—actually, I am more familiar with the *Bast* case, which involves Richard Bast, a Washington private investigator and purveyer of electronic equipment. And as a private investigator, I handled the California phase of that investigation and I must say I am not very happy with the way the prosecution or the investigation was conducted by the Government. And in that particular case a gentleman in Gardena, Calif., got ahold of Mr. Bast and asked him to send him literature on a very small recorder that he had. Now a recorder is not necessarily primarily useful for electronic eavesdropping. Recorders are used by businessmen and they carry them in their pockets on a plane or travelling. And this particular one had some 50 words of sales copy on it. And the one word that apparently was the crux of the Government's case was that he used in the course of that sales pitch the word "secret". And the way they got the literature to be sent interstate was to have this man in Gardena, Calif., ask for it. And then there was a telephone conversation in which the man asked him if he could put VOR's on it, which are the voice operated relays, and in my opinion, take it one more step towards the clandestine. And I think the evidence is clear that Bast said, if you want to do that, you do it on your own, you know, here is the instrument, here is the price.

And my investigatiton of that case was that I went down to see this man. Unfortunately, he was the victim of a homicide perpetrated by his son, as the police would say, days before. But at any rate it turned out that this man, according to the tapes that I did get on the case, had been working as an agent of the FBI and I think it was a case of borderline entrapment.

So here was a case that to me was very marginal. It didn't go to the heart of the problem of bugging and tapping and yet, this prosecution had been persisted in by the Government. And I think that we still haven't got a case that very clearly brings out the aspect of surveillance that we are talking about in these kinds of hearings.

Mr. KASTENMEIER. I have some other questions, but I want to yield to my colleagues because I want them to have the opportunity to ask questions as well. The gentleman from Massachusetts, Mr. Drinan.

Mr. DRINAN. Thank you very much, Mr. Chairman. I would like to get back to the question I raised this morning in that you have extensive background in this whole area. How essential or indispensable is wiretapping to the effective and successful prosecution of the criminal law?

Mr. TURNER. My experience is that if it was done away with, if it was abolished totally, that I doubt that there would be a drop in the bucket impact on the law enforcement in this country.

Mr. DRINAN. Can we make it a bit more precise than "a drop in the bucket"?

Mr. TURNER. Well, I listened in on these, and as I said before, I don't know how many thousands of hours I listened in on people's lives being trotted before me. And I agree that a lot of it was for so-called security purposes, but even from that standpoint, from the standpoint of that type of intelligence-gathering, my opinion was that it wasn't worth it, either in terms of the logistics, the money, the time involved, or in the constitutional or human terms, in terms of invasion of privacy involved.

Mr. DRINAN. Has anyone done a really hard, empirical study on how many cases have really been prosecuted successfully because, and only because of, wiretap evidence? Or in the alternative, a study that if they had wiretap evidence, they would not have lost the case?

In other words, the burden is on the Department of Justice and the FBI I would assume, but they don't seem to say that burden is on them, and they go in and they get all of these warrants about wiretaps, about which we never really hear.

And in your judgment, would you restate it in scientific terms or in percentage terms that far less than 1 percent of all of the cases might be lost or even less than that?

Mr. TURNER. Well, yes, I think that really there were some prosecutions initially when this was authorized, but I think now with all of the publicity, you know, we have published a pocket-book edition of "Sam the Plumber's Intercepted Wiretaps" and all and it would seem to me that anybody indulging in that type of activity of an organized nature and using the telephone as a means of communication and furtherance of a criminal act is awfully stupid or at least if he doesn't use a voice scrambler, he is stupid. There are just other ways of communicating in code or something.

And I think that at this point the real victims of continued wiretapping and electronic surveillance are not going to be what you would call the heavy organized criminals, but the common citizen and people who are at maybe the first time in.

Mr. DRINAN. I have had extensive discussions and given lectures over the years on this precise subject and I always say to law enforcement officials or rather ask them, I always ask whether or not this makes them lazy. The fact that they can in fact wiretap, does this make them less resourceful in seeking alternative ways of discovering clandestine activity.

Mr. TURNER. Well, I think back around 1938 or so, J. Edgar Hoover said he was against it because it was the lazy man's tool. And he of course turned around and was for it later on. But in any event, I agree that it is probably a short way of doing it in certain instances to go about it, and it does, if you get this kind of a short cut, it does create a legion of law enforcement officials who are not versed in conventional methods of investigation and lose their skills. That is true.

Mr. DRINAN. One further question. When did you leave the FBI?

Mr. TURNER. 1961.

Mr. DRINAN. Are you in a position to make any judgment whether wiretapping has become more utilized or less?

Mr. TURNER. Well, after 1961, when Robert Kennedy came in the Justice Department, there is no question that FBI wiretapping increased, simply because they had been behind on their intelligence on organized crime and Kennedy wanted answers to what was going on in the criminal netherworld. The embarrassment of the 1966 disclosure of FBI intelligence installations in Las Vegas and the resultant lawsuits, the civil suits filed by the victims, against the Central Telephone of Nevada and all, I am sure again brought about a temporary curtailment. I am sure that when the hearings come on, that there is considerable pulling back of the electronic surveillance, but I think that if we look at it in long-range terms, I think that the tool has been so commonly used throughout law enforcement that there is little hope of it being cut back unless there is some law that says it should be and some effective way of doing it.

Mr. DRINAN. Did I understand you to say that the FBI would pull back on electronic surevillance because of these hearings here?

Mr. TURNER. No, I said it is my feeling that when these hearings are held, like for example when the Long's Subcommittee of Administrative Practices and Procedures of the Senate had hearings, I have a feeling then that they were cut back. I have had some feedback from inside the FBI that when the heat is on, that "we will pull them out" and then they will start them up again when the heat is off.

Now these are the kinds of things that I can't say from direct experience. I wasn't there if and when they pulled them out, but it is the kind of thing I say that, if this type of activity is going to be permitted, if our laws are going to be permissive in respect to wiretapping and bugging, that the enforcement has got to be in the hands of some totally independent investigative group that has total access to the facilities and personnel of the wiretapping and eavesdropping people.

Mr. DRINAN. Maybe we just should keep the hearings going indefinitely?

Mr. TURNER. Could be. That is one way of doing it.

Mr. DRINAN. Thank you very much.

Mr. KASTENMEIER. The gentleman from Illinois, Mr. Railsback.

Mr. RAILSBACK. I notice in your statement an anecdote about Jessica Mitford, who was also the subject of a tap. I don't think you mentioned that in your testimony. What was that incident about?

Mr. TURNER. I mentioned that back in the early 1950's I was assigned to the wiretapping plants in the San Francisco Bay area that the FBI had at that time. The story would be this, that a few years ago I was at a cocktail party in San Francisco and I heard this very distinctive woman's voice and I couldn't place the face. I could not associate the face with the voice. So I went over and introduced myself and sure enough it was Jessica Mitford and sure enough the voice I had heard so many times so long ago on the wiretaps

that we had on Jessica and Bob Trufaft, her husband who is a civil liberties attorney, was exactly that.

Mr. RAILSBACK. I'll be darned.

I guess that is all I have, Mr. Chairman.

Mr. KASTENMEIER. I know that you have written a number of books or articles on law enforcement, privacy, and electronic eavesdropping. Have you been personally subjected to harassing by the Bureau or others as a result of your rather open and candid disclosures about their operations and others'?

Mr. TURNER. Yes, I have. On two occasions I was notified by an editor, Murry Fisher, of "Playboy," that the FBI had been up to see the "Playboy" editors about articles that I had submitted to "Playboy" directly for consideration for publication. Both of the articles dealt with the FBI. And it was a mystery to me as to how the FBI knew "Playboy" held the articles since unless somebody inside, the mail clerk or somebody inside, tipped them off, they wouldn't know. But at any rate they showed up and Mr. Fisher told me it was very obvious that the idea was to intimidate "Playboy", not to publish them. The same thing happened at "Saga" magazine on one occasion when I published "Hoover's FBI" in 1970. I went on the usual promotional tour that the publisher puts you through. And at that time the FBI distributed an anonymous so-called fact sheet on me, which was carried by an agent, unsigned, no letterhead, carried by the agent to the various producers. Their impression was that it would hopefully keep me off the air.

In Philadelphia, Tom Snyder, who is now at the "Tomorrow" show, said "Well, I knew what kind of a suit you would be wearing, I knew you would wear a gray suit."

The FBI had been there, you know, and they told him I was coming in there from Pittsburgh. So whenever I do get involved in publications that apparently they disapprove of, I do find there is that kind of harassment or surveillance.

Mr. KASTENMEIER. There is a vote on and we will have to again recess for about a period of 15 minutes. We will resume at 2:30. There are other questions we might ask of you, Mr. Turner, but I will not hold you any longer. I think that will conclude our inquiries of you.

We might like to keep in touch with you. To the extent that we are dependent on information and factual data, and sometimes merely allegations, to learn what does exist, your appearance here today has been most helpful and the committee appreciates it.

Mr. TURNER. Thank you, Mr. Chairman.

[Mr. Turner's Statement follows:]

STATEMENT OF WILLIAM W. TURNER, A FORMER FBI AGENT, PRIVATE INVESTIGATOR, AND AUTHOR OF SEVERAL BOOKS

OUTLINE OF PROPOSED TESTIMONY

Background.—After service in the Navy during World War II, attended Canisius College, graduating with B.S. in Chemistry 1949. Entered FBI as special agent in 1951 at age 23, serving for over ten years before being ousted for asking for Congressional review of Hoover's policies. Posted to five field offices, worked predominately criminal and counterespionage. Designated as Inspector's Aide, a kind of junior executive duty, and a Sound Man, a euphem-

ism for a graduate of the FBI's school on bugging, tapping and burglary. Since leaving the FBI, have written numerous articles for the legal press on police science topics, edited the *Police Evidence Library* series, authored a number of articles in various magazines and newspapers, written five books on popular subjects, e.g. *The Police Establishment* (Putnam's); *Hoover's FBI* (Sherbourne Press; Dell); and *The Ten-Second Jailbreak* (Holt, Rinehart & Winston); as well as a mail order book *How to Avoid Electronic Eavesdropping and Privacy Invasion*. Possesses a California private investigator license, working primarily for attorneys on defense cases.

Training and Experience in Electronic Surveillance.—First involvement was in San Francisco FBI office in 1952–53 when assigned to the monitoring plants there. Description of the plants and how they operated, who was tapped, e.g. Al Richmond of the Daily People's World and the Yugoslav consulate. Anecdote about Jessica Mitford, who was also the subject of a tap.

After some mishaps, including a police raid on a monitoring plant suspected of being a bookie joint, FBI plants were relocated inside the field offices.

In April 1958 was selected to attend the Sound School held in Washington. Similar to schools conducted by the Treasury Department agencies, CIA and military intelligence. Little discussion of Constitutional issue—simply told that FBI tapped under two justifications: (1) that President Roosevelt gave executive authority and no succeeding president has descinded it; and (2) that the element of disclosure in the Communications Act of 1934 was not violated because information obtained was not disclosed outside the Justice Department. Instructor added that the act was intended not for the FBI but for telephone employees in league with private detectives.

We were told that the authority for any device connected to a telephone must come from the A.G., but that the Bureau installed microphone surveillance on its own authority. Thus the announced number of wiretaps—always around 100 nationwide—was only a part of the picture, not the whole. Illustration: once instructed to pull out a tap and install a mike, keeping the books in balance but necessitating a burglary.

The training sessions were conducted mainly in the Identification Building. There was a practice room where we planted bugs in walls and taps on the phone. We went down to the FBI radio station in rural Virginia to practice pole climbing. In an attic of the Justice Building there was a workshop where agent George Berley taught us how to make lockpicking devices and use them.

Back in Seattle I employed these skills, handling security of the office communications as well as installing taps and bugs. Recall taps on relatives of suspect in Coors kidnapping, CP functionaries, security subjects. Permanent installations involved the leasing of a line from the telephone company under some cover name such as Federal Research Bureau. The telco had to suspect the purpose since no hookup was ordered at either end—the subject's pole box where the jump was made or the FBI office building where the plant was. Liaison was maintained with the Special Agents of the telco. They would assist with arrangements, furnish information from the subscriber's cable card that was necessary to install the tap, and notify us if telco personnel found a tap or bug that we put in. Also they would place a recorder on a subscriber's line terminals in the Central Office for short periods of time. Most telcos around the country cooperated lavishly with the FBI.

Taps and bugs were supposed to be approved by Washington. However, there were "suicide taps," so called because the person installing them without permission was liable to disciplinary action if caught. The problem was that the Bureau trained and equipped people to use the technique, and couldn't hope to control the situation from Washington.

Burglaries.—The FBI alluded to burglaries as "black bag jobs," after the tool kit usually taken along. When I entered the Bureau in 1951 BBJs were a standard technique, along with tapping and mail covers and trash covers. They were conducted for two main purposes: (1) to install a microphone inside, and (2) to gather intelligence and photograph documents. The BBJ is different from the conventional burglary in that nothing is removed and every effort is made to disguise the fact that entry was made. I participated in a number of BBJs, including a 1957 burglary of the Japanese Consulate in Seattle. In that operation George Berley flew out from Washington and used radioactive cobalt to gradually photograph the locking mechanism of the safe. The contents of the safe were photographed and returned in place.

Elaborate measures are taken to ensure the security of a BBJ. The premises is thoroughly "cased" to make sure the regular occupants' movements are known. Tails are put on them at the time of the BBJ. An agent sits at the police radio console to make sure complaints of a burglary in progress are not answered.

FBI agents who made a specialty of BBJs were rewarded for their risks in the form of meritorious cash awards.

Telephone Taps.—Description of a telephone tap. Two kinds: direct and inductive. A tap-transmitter in which a phone line is tapped and the conversation sent over the air to receiving point. Security because if found, not traceable (Exhibit of such a device).

Explanation of multiple appearance and the security it affords a tapper. Cooperation of phone company necessary; otherwise difficult to determine where the multiple appearance is located.

Problem of control: a few years ago when Hoover contended there were less than one hundred taps nationwide, the Washington Post disclosed that the FBI had 450 "special service" leased lines feeding into the Washington field office from all over the city.

Microphones/Bugs.—These fall into two categories: wired and wireless, or the bug-transmitter.

The wired simply means that the microphone is connected to the listening post by a run of wire. Example: installation in Seattle were picked lock to enter dwelling, replaced the telephone connecting block with one hand-fabricated by FBI lab containing miniature microphone, ran fine wire down through basement to connect with special drop wire in which wire for mike built in and invisible, from drop wire terminal in pole box a bridge was made to a leased line. Trouble with commercial radio station nearby interferring—aerial wire acting like antenna. So designed low-pass filter to filter out the radio frequency.

The wireless type is the most common. It can be planted stategically, and if discovered is not traceable to the eavesdropper. He is simply out the $50 or so a decent one costs. The wired type is more vulnerable to detection because of the necessity for wires to be run in the premises and leave somewhere. Example: Polish Consulate, Chicago.

Exhibit of a bread-and-butter, inexpensive bug-transmitter. Depending on surroundings, transmits a hundred feet or so from room. Ordinary pocket FM radio will pick it up. More batteries, more power, greater range. Broadcast time limited to life of batteries, necessitating replacement. Eavesdropper may use radio switch to turn on and off and conserve power. May use repeater station, say, buried in yard. Or may pirate current from phone circuit or house power.

Hit-and-run eavesdropping. Stethoscope-like device pressed against wall. Very effective is the spike-mike. Exhibit: this one is disabled so not primary useful for anything, but the species was specifically named in the legislative history of the 1968 law as being primarily useful. Other bugs may be used as baby-sitters, burglar warnings, etc.

State of the Technology.—Much has been made about futuristic devices and their deployment throughout the land. For instance, the olive-in-a-martini transmitter. Such a device does exist, but is quite impractical. It will transmit only a few feet, and without much clarity. The CIA is said to have a LASER device that aimed at a window will pick up the room conversations from the minute vibrations of the glass pane. Tiny integrated circuits developed for the aerospace programs don't auger well for the future of privacy. However, the cost and uniqueness of much of this exotica renders it available only to government agencies, not the average eavesdropper. It should be pointed out, however, that there are electronic engineers that moonlight making very sophisticated devices.

Prevention and Detection.—If a subscriber suspects a tap he can have the telco conduct an inspection, but if a law enforcement tap is in the telco usually will not advise him. Most law enforcement taps are in the telco Central Office, which makes detection next to impossible. Contrary to mythology, a properly installed tap will not cause clicks and noises.

The citizen can conduct his own preliminary check for devices, checking his premises for such things as fresh plaster marks, alien wires, and antennae wires of a bug-transmitter.

Also, he can hire—at substantial cost—a professional "sweeper." Beware of some who advertise their services, show up with simply a "hound dog" or

field strength meter, and declare the premises "clean." Some unscrupulous operators have even planted bugs, then "discovered" them, as a prelude to a pitch for their periodic services. A truly professional search requires some $10,000 worth of equipment. It should also be noted that bugs that can be remotely turned on and off are very difficult to detect. Also, the eavesdropper may plant a decoy bug that is easily found, lulling the target into a false sense of security.

Beware of "gifts" that might contain bugs, of repairman and utilities men who want entry to the premises, of salesmen who drop by and leave a briefcase in the conference room.

Mr. KASTENMEIER. Until 2:30, the committee stands in recess.

[Brief recess.]

Mr. KASTENMEIER. The subcommitte will come to order for the resumption of the afternoon hearings. I apologize to the witnesses for the frequent interruptions. Other members will join the panel, I am sure, and in the meantime I would like to continue with the next two witnesses who are Mr. Leon Freedman and John Shattuck, representing the American Civil Liberties Union.

Both Mr. Friedman and Mr. Shattuck have had broad experience in the area of wiretapping and electronic surveillance. They have been active in civil suits. Particularly, I am thinking of those against the government for recovery of damages for illegal eavesdropping. And in other regards they are very deeply interested in the issues that confront this subcommittee.

We welcome you both, and you may proceed as you wish. We have a copy of your testimony, which is some 19 pages. However you care to proceed, you may.

TESTIMONY OF LEON FRIEDMAN, ESQ., AND JOHN SHATTUCK, ESQ., OF NEW YORK, ON BEHALF OF THE AMERICAN CIVIL LIBERTIES UNION

Mr. SHATTUCK. Thank you, Mr. Chairman. We are very grateful for the invitation to testify on an issue as important as this one to the ACLU. As you have noted, we have a joint statement and both Mr. Friedman and I will be participating in this. And I will lead off, with the Chairman's leave, because I have a court appearance at 3 o'clock and I may have to leave the balance of the testimony to Mr. Friedman.

As Congressman Drinan noted this morning, the ACLU for more than a decade has been strongly opposed to all forms of wiretapping and electronic surveillance. We believe that the disclosures over the last 2 years with respect particularly to national security, to warrantless wiretapping, have underscored the original wisdom of our policy. In our testimony today we will attempt from the point of view of lawyers who are actively engaged in wiretapping litigation, to catalog national wire security tap abuses, and our principal focus will be a civil law suit in which we are representing Dr. Morton Halperin and his family. He was the target of a 21-month national security wiretap from May of 1969 to February of 1971, of which I am sure he will testify himself at further length.

His tap was one of the 17 so-called "Kissinger taps" purportedly installed to trace news leaks from the White House. And in our view, these taps illustrate some of the worst national security abuses.

Our statement, as you will notice, is divided into three parts. First is an explanation generally of why the ACLU is opposed to all forms of wiretapping and why the statutory regulation of wiretapping under the Omnibus Crime Control and Safe Streets Act is really insufficient to regulate or rather to deal with the deficiencies which we have identified. Second, a description of national security wiretapping and why it represents the most serious abuse and invasion of constitutional rights of any of the various forms of wire- with renewals possible upon probable cause, make it possible to to cure the national security abuses.

I will attempt briefly to outline why it is that we are opposed to all forms of wiretapping and Mr. Friedman will then describe the civil suit brought on Dr. Halperin's behalf and a number of other national security wiretap cases. And then, if time permits, I will return with respect to some of the proposals that we see are necessary in this area.

The fundamental reason why we are opposed to all forms of wiretapping is that the major wiretap technology is such as to make the practice an inherently unreasonable search and seizure regardless of any safeguards that might be imposed by law. It is far more intrusive than a search of a person or of a house because it is indiscriminate; it picks up all conversations.

I think Senator McClellan has illustrated this point without intending to by pointing to the wiretap statistics as evidence of the kind of controls that Congress has brought to bear in this area. And I don't think they demonstrate any controls at all. Senator McClellan pointed out that in 1972 the Justice Department's statistics showed that an average tap intercepted 1,063 conversations among 66 persons for an average of 3 weeks. This is hardly a limited search.

The warrant procedure of title III merely underscores the breadth and intrusiveness of wiretapping. First, it is essentially unlimited even under the statute. The unrestricted 30-day renewal arrangements allow indefinite tapping.

Second, contrary to the general fourth amendment law, which requires that a search warrant particularly describe the things to be seized, wiretap warrants cannot comply with the particularity requirements, because it is so difficult to describe conversations which have not yet taken place as those conversations which are to be seized. And the statute merely says that the warrant must describe "the type of communication to be intercepted", which really doesn't amount to very much.

Third, there is no prohibition in the statute against intercepting privileged communications. And it is no coincidence, therefore, that over the years the wiretap method has been one of the principal ways of invading the lawyer-client relationship. There are a number of instances of this in our testimony.

Fourth, both the wiretap statistics and the legislative history of title III demonstrate we believe that the principal purpose of wiretapping is not the investigation of specific crimes at all but in fact is general intelligence gathering or preventative surveillance, or really

the interception of speech pure and simple without regard to its probable criminality. So the inherent nature of the practice is really what it is that drives us to the position that it in and of itself violates the fourth amendment.

And since national security taps by definition are used both outside of title III and outside the scope of any specific criminal investtigation, they are necessarily worse than the taps that are covered by the 1968 act and represent the worst forms of abuses.

I think Mr. Friedman can proceed with the specifics of some of the cases under national security wiretapping.

Mr. FRIEDMAN. Under national security wiretapping the few procedural safeguards that exist under title III are just swept under the rug altogether. In order to start a national security wiretap, someone in the government simply writes a memo or calls the FBI, since it is the FBI that actually administers the tap, and they are the ones who are to justify——

Mr. KASTENMEIER. I take it you have learned how these things transpire and so this is really your acquired knowledge on the subject of what initiates national security taps as opposed to title III taps?

Mr. FRIEDMAN. That is correct. Let me just say this. There are two levels of the things that we know. There are matters which we know from public record documents and there are some other matters which we are under a court order not to discuss. And so what we will testify here to is as to those matters which are in the public record and which appear in the court records.

There are some additional matters, some additional material, actually, which we have not even seen yet, that we know something about, but we are under a court order not to disclose that additional material.

And so I think we have a pretty good idea of what happens on the basis of our own litigation and what is a matter of record.

Mr. KASTENMEIER. Again, I must say I apologize but we are now called in for another vote. That is the second bell. And if it were a quorum call, it might be another matter, but a vote we will be required to go to. I would ask my colleagues, however, if they would promptly come back and we will recommence the hearings hopefully in 10 minutes. Just go over and vote and come directly back.

I realize, Mr. Shattuck, that you may have to leave. If that is the case, our apologies. But the subcommittee will stand in recess for 10 minutes.

[Brief recess.]

Mr. KASTENMEIER. The subcommittee will come to order. When we recessed, Mr. John Shattuck and Mr. Friedman were testifying.

Mr. FRIEDMAN. Mr. Shattuck had to go to a court appearance.

Mr. KASTENMEIER. Mr. Friedman, you may continue.

Mr. FRIEDMAN. Yes, I just wanted to go over the procedures that are followed in national security wiretapping and how the government starts the procedures and what steps they take. This is obtained primarily through our discovery in the Kissinger tap case in which we have questioned the government at some length about the pro-

cedures that are followed. And the first thing is that justification has to be offered for a national security tap. And what we found in the Kissinger taps and in other cases—

Mr. KASTENMEIER. Are these merely guidelines?

Mr. FREIDMAN. No, these are just internal procedures. The government itself has established some kind of procedure which it can violate on its own. And in fact, in national security taps generally there is a justification offered to the Director of the FBI as to why a tap is necessary. And then he in turn, based upon those justifications, will ask for an authorization from the Attorney General. And the Attorney General is supposed to himself personally approve any such tap. That is the procedure that the government has established on its own in order to go forward with national security taps.

Mr. KASTENMEIER. Mr. Friedman, when you say the government though, can you be more particular than that? Who within the government?

Mr. FRIEDMAN. Well, the Justice Department, the Attorney General.

Mr. KASTENMEIER. The Attorney General?

Mr. FRIEDMAN. The Attorney General. John Mitchell was very proud of the fact, as when he testified before the Ervin committee, that he had established a 90-day rule so that in a national security tap, they must come back to the Attorney General every 90 days in order to get additional authorization.

Now that is the story that they tell, but in fact it doesn't happen that way. The justification that is offered is either very thin or it can be nonexistent. We quote in our statement from the fact that Mr. Ruckelshaus said that when a national security council request is made for a tap, there is no justification offered. They say "we want a tap" and that is it. And Senator Case asked him: "Could that elaborate procedure be avoided by having a Director get Henry Kissinger to say 'let me have the dope'?"

And Mr. Ruckelshaus answered "sure".

And Senator Case said "In other words, the authorizing document does not necessarily, in itself, tell the full story."

Mr. Ruckelshaus answered: "That's possible."

So even though a justification is supposed to be offered, in fact it doesn't always happen that way. And the minute you are dealing with internal justifications within the government, they can simply say "We don't to follow our own procedures in this case".

Now what about this 90-day rule? Well, the 90-day rule was not followed in the Kissinger tap case at least with respect to Dr. Halperin's tap, although Mr. Mitchell was very proud of this 90-day rule. In fact, there was only one authorization for the tap on Dr. Halperin, and that single authorization continued the tap for 21 months and there was never any stop to it. Based on the original authorization that John Mitchell says he doesn't remember signing.

So these internal standards that the Justice Department had established are in fact not binding at all even on the Attorney General and the Director of the FBI.

Now we cite also the fact that the justifications that are offered for national security taps are absolutely absurd at times. Now Martin

Luther King was tapped. His home phone was tapped. His office phone in Atlanta was tapped and another office phone in New York was tapped. Why? Because he supposedly had associates, he supposedly had two Communists or alleged Communists on his staff.

Now the question is why didn't they tap the alleged Communists? Why did they have to tap his phone rather than the people who were supposedly improperly influencing him? And the answer was not comforting. J. Edgar Hoover said to Attorney General Robert Kennedy: "We want to tap Martin Luther King because there may be improper Communist influence upon him."

And the tap was made upon Dr. King's phone, and not on the alleged Communists' phones.

So this business that there should be a justification for a national security tap, which you know sounds very good, and the fact the Attorney General says "We have our own way of handling this" sounds very good, but it doesn't work because the justifications offered can be absurd when offered to an outsider, but they are not observed when they are offered to insiders within the Justice Department and the FBI.

And the Halperin tap and the King tap are just two examples of this.

One other thing that emerges from the analysis of the national security tap is that there may be situations in which the Government can go and get a title III tap just as well as a national security tap and have to follow the requirements of title III, but if there is a choice at all between going under a title III tap and going under a national security tap, they will always go under a national security tap. Why? Because then they don't have to get a warrant, they don't have to follow all the housekeeping, all of the warehousing procedures of title III and they don't have to follow what few procedural safeguards exist under title III. And this has been consistent. This has been a consistent pattern along. If they can avoid a warrant and avoid title III, they will do so.

And we cite a number of cases in our testimony, Mr. Chairman, showing this. And the Jewish Defense League situation, where there were taps on Russian diplomats up in New York, is an example. They could have gotten a title III warrant if they wanted, but instead they decided to go under national security because as far as the Government is concerned, this allows them to cloud their trail. They don't have to keep the records, they can destroy the tapes at the last minute, they don't have to give them to the defendant, they don't have to follow the recordkeeping procedures under title III. They can just go ahead and tap without any procedural safeguards.

Now we outlined in our testimony what procedural safeguards are lacking in a national security tap that do exist in title III. We are not saying that title III is wonderful and should be followed, but there are some things that title III has that a national security tap does not have.

For instance, No. 1, there is supposed to be a time limit on a Title III tap. There is supposed to be 30 days which can be renewed except you have to go into court each time this happens. Under a national security tap there is no limit.

Under Title III, there is supposed to be a minimum invasion of the privacy of the person who is to be tapped. That is to say, there is a requirement that if the conversation is not related to the purpose of the tap going on, they are supposed to switch it off. In a national security tap there is no switching off because everything that the person says is conceivably something that could bear on national security and therefore the tap stays on and political conversations are intercepted, sixth amendment rights between counsel and a client may be intercepted, and there is absolutely no requirement of minimizing the scope of the tap.

Now all of this is laid out in the Kissinger tap case itself. What kind of conversations were interecepted and what kind of limitations were set in those particular cases? And what we found in those cases was that there was only a single authorization. As I just mentioned, they never went back to a court. They never went back to the Attorney General. And they simply continued the tap for a 21-month period.

No. 2, the kind of conversations that were intercepted, these were political conversations, conversations that related to a political campaign then in progress, conversations relating to articles and a political stand that Dr. Halperin was taking at that time. All of this was intercepted. It was intercepted, and as we know from public testimony, summarized on a regular basis and sent to the White House for them to use in any way that they chose.

The Government erased all of the tapes of the original taps and we have to rely on transcripts, and we don't know how accurate those transcripts are.

And so what happens in national security taps is that there is an absolutely massive invasion of the privacy of an individual and a massive invasion in an area in which protection is absolutely essential. Political conversations are intercepted in national security taps, conversations relating to protected first amendment activities, criticism of the Government, criticism of the Government's policies that may be involved. And all of this finds its way immediately back to the White House, which can make very substantial use of this material in a political campaign, as it did in Senator Muskie's campaign—finding out materials, finding out what consultants were saying that could be useful in the campaign, and sending it back to the political advocates in the White House that might find it useful, and all in the name of national security. Because once the tap is installed on some vague national security justification, there are no restraints, and a justification that is not even offered to a court. It is just offered to themselves. You know they say, "is there some national security reason why we can justify the tap" and in the Halperin case they said that there was a leak of national security information. Who had this information? There was a list of 13 people gotten up. To whom was this information leaked? Four newsmen are gotten up. The names of four newsmen are gotten up. And those people are tapped for an indefinite period of time; for as long as the Government, as long as the White House, as long as the FBI, as long as the Justice Department, thinks that they can get some value out of this material.

And in Dr. Halperin's case, it continued for 21 months, and there was absolutely no stop until the Government decided that it in effect had had enough.

Now we talked about the different invasions of constitutional rights, about the first amendment rights that are invaded, the mass invasion of fourth amendment rights, the invasion very often of sixth amendment rights. Agent Turner this morning disclosed the fact that a civil liberties lawyer in San Francisco had his home phone tapped for a considerable period of time just because the Government or the FBI could think of some national security reason why they might be valuable. And as far as we know, Arthur Kinoy, who was another lawyer for civil liberties groups, his phone was tapped. There were 21 separate interceptions of his conversations extending over a period of 20 years. In the Chicago conspiracy case it turns out that client-lawyer conversations were intercepted. So that once you are armed with this catchall of national security, which isn't even limited to a particular kind of crime, once you can offer some vague justification for national security, then all of these rights can be trampled on.

Now the question is, would a warrant procedure save the situation? Would the requirement of getting a warrant for a national security case, would that help? And our answer is, as long as you have this vague notion of national security which is ill-defined, which is so illusive, a warrant procedure is not going to be of any sifinificant help. It is some help. It is some help in terms of record-keeping. It is some help in terms of finding out what the Government did afterwards. It may be of some help in making sure that the documents and the tapes are preserved, so that, if there is a search later on, there might be some redress, but it is no help at all if you maintain this vague and ill-defined notion of national security and foreign intelligence. Because at that point the Government is going to be able to go into court and say to a judge, just as it did in the Kissinger wiretap case, that there is a massive leak of national security information and here are the 13 people who have access to this information and they want to be able to tap their lines. Now that is very plausible. That is a very plausible argument. It is a very plausible justification. Is a judge going to say "I want to know more about it?" Is he going to put them to the proof?

You know, it sounds good. It sounds like a good story. And therefore they will be able to secure that warrant and theoretically they can come back again and again for extensions of the warrant and be able to make all the invasions of the first, fourth and sixth amendment rights that we have talked about up until now.

So the real problem is not so much the warrants, although it may be some improvement, as this vague notion of national security.

And the answer is you've got to attack national security as such. This magic term that has been used to justify the Kissinger taps, and has been used to justify breaking into Ellsberg's psychiatrist's office, and used to justify a wiretap of Dr. King, and used to justify a coverup of the Watergate break-in, has to be defined. National security just creates blinders as far as the Government is concerned.

And Congress should not be in a position of justifying and authorizing the kind of national security we have been talking about up until now.

Mr. KASTENMEIER. If someone asked you to define national security, in terms that would help set forth when and under what circumstances a warrant for such a matter might be obtained, how would you do it?

Mr. FRIEDMAN. Well, the answer to that is that title III itself specifies exactly the kinds of crimes that we are talking about.

Mr. KASTENMEIER. Yes, and mentions some of those.

Mr. FRIEDMAN. And mentions some of those. And so, I mean, if Congress is interested at all in getting into the question of national security taps, they can very well say that all the national security crimes that we have are already under title III, and no other kinds of taps shall be permitted except those already covered by title III. And that would take into account exactly the problem we are talking about, that is, espionage, sabotage, and so on. We went over the list of the crimes in 2516 and actually one-third of them relate to national security issues already so why should there be anything beyond the requirements already contained in the act?

Mr. KASTENMEIER. Mr. Friedman, what is the Government's position in this matter? Why do they insist that there are national security taps which are authorized pursuant to some other power external to title III?

What is the Government's position on this as opposed to your position?

Mr. FRIEDMAN. Well, again, we've got this in answering briefs from the Government, that the Executive has the constitutional duty to protect the Nation against foreign attacks, against foreign intelligence activities.

Mr. KASTENMEIER. Pursuant to law?

Mr. FRIEDMAN. There is a catch-all and I guess it is 18 U.S.C. 2511 which says that nothing in this act shall bear on the Executives's power to protect the national security against foreign intelligence activities, whatever that might be.

Mr. KASTENMEIER. That is the answer then, that is the exception they resort to?

Mr. FRIEDMAN. 2511 does talk about some exceptions which may or may not exist. Now the Supreme Court has already held that Congress did not authorize any of these exceptions. All Congress did was recognize there may be such an exception. And if there is such an exception under the Constitution, we are not dealing with it with this legislation.

I think the wording of the section says that if there is such a thing as a foreign intelligence exception, if there is such a thing as dealing with foreign spies when they come in, or gathering general information about foreign activities, we are not dealing with it at all in this legislation.

Now our answer to that is that the Government has used that loophole too widely already. They justified the tap on Dr. Halperin

not on the ground that there was an internal security problem. They justified it in their very words in their brief, which we quote here, by stating that a foreign government by reading the newspapers will be able to find out national security information. There argument presumed that if a member of the Government talks to a newsman and the newsman publishes this information in the press and the foreign government can read this information in the press and gather foreign intelligence activities, it comes under national security. So therefore it is necessary to tap Dr. Halperin and newsmen in order to protect against a foreign government's finding out information on national security. That is the way this was done.

So the thing is, you give them an inch and they will take a mile.

Mr. KASTENMEIER. I would think they might have trouble establishing that sort of approximate nexus.

Mr. FRIEDMAN. But they did it. That is the way they did it. And if they had to go to a court in order to justify a warrant, presumably they would be able to tell a very plausible story and get a warrant for that.

Mr. KASTENMEIER. But in other words, and the reason this colloquy is useful, Senator Nelson's approach may be unavailing, even if it becomes law, if in fact resort is still made to 2511, subsection 3?

Mr. FRIEDMAN. Well, that might be because the Government's position is they have an inherent power to protect the Nation against foreign intelligence activities.

You know there is the famous debate between Senator Ervin and John Wilson and John Ehrlichman when they said "Where did you get the authority to break in to Ellsberg's psychiatrist's office?" And they pointed to that section of the law. And they said: "2511(3) gives us that procedure, because Congress recognized that we have the power to protect ourselves against foreign intelligence activities."

That was the justification for that break in to Dr. Fielding's office. The Government, you know, they may be sincere in claiming that these kinds of taps are necessary. But our point is that unless you close that door, it can be used for just about all of the purposes that we have outlined here today.

Mr. KASTENMEIER. Are you suggesting we might repeal the section?

Mr. FRIEDMAN. Absolutely, or narrow it to specifics. In other words, if it were narrowed to foreign agents, or foreign nationals of a specific kind engaged in certain kinds of activities, perhaps that might be a way of dealing with it.

Title III we feel really covers whatever genuine national security issues the Government is concerned about. But to have any kind of loophole at all is going to allow the Government to use that to tap people like Martin Luther King, tap its political enemies, tap people in the Government that it wants to know what they are doing, tap newsmen. And the Government has in fact used it for that purpose. So it will tap all of that under this magic rubric of protecting the Government against foreign enemies. So unless there is some very

specific kind of definition of "national security" that goes along with the warrant procedure, a warrant procedure is not going to be much help. It will be some help. I am not saying that it won't be any help. I mean, now there is nothing at all. So anything that closes some of these doors would be helpful, but it is not a terrific help at all unless there is some effort to close that door of national security.

Mr. KASTENMEIER. And in order to do that, you might merely narrow that section rather than to try to define "national security" which might be rather a futile exercise.

Mr. FRIEDMAN. Well, I mean our order of preference is to have no wiretaps at all. If there are to be wiretaps, it should be under title III only because that covers whatever legitimate national security considerations we have. But if you want to go beyond that to some kind of foreign intelligence exception, that really must be defined very specifically and the door that is left open in 2511(3) has to be narrowed.

Mr. KASTENMEIER. Of course 2511(3) may be repealed or amended——

Mr. FRIEDMAN. Exactly.

Mr. KASTENMEIER [continuing]. Or we might potentially ban wiretapping completely, but the President still would rely on the philosophy contained in section 2511(3) that the Congress could not impair his constitutional power to protect the country against foreign enemies, and that he would be free to use whatever devices were at his command to do so notwithstanding the enactment of the Congress.

Mr. FRIEDMAN. I think that if Congress declared as its policy that we want the President to protect against foreign attack, but that we believe that title III gives him whatever powers he needs, I think it would be very difficult for him to claim that Congress' judgment and my judgment are different and I am going to take my judgment on this.

Mr. KASTENMEIER. We have had the debate and the dialogue on Presidential power in many contexts. Two or 3 years ago when we repealed title II of the Internal Security Act, which apparently authorized the maintenance of detention camps in America, the question arose that the President as Commander-in-Chief, within an emergency or war situation, might still have the constitutional power to perhaps maintain such institutions. We tried to suggest he did not, but we granted the argument continues, notwithstanding enactment of that law.

Mr. FRIEDMAN. But the U.S. Supreme Court in its unanimous decision in the *Keith* case suggested that there is no inherent Presidential power to tap for domestic subversives on a national security basis. It was a unamimous decision, with Justice Powell writing the opinion. And that certainly suggests that the Supreme Court is ready, willing and able to knock down the notion of inherent Presidential power once Congress has spoken in this area. And it is because Congress spoke, I think, that the Supreme Court was willing to go along with the kind of judgment that the Congress made.

Mr. COHEN. Would the Chairman yield?

On the *Keith* decision, wasn't it simply that they ruled that authorization for a wiretap in a domestic security case by the Attorney General without judicial sanction of the fourth amendment was illegal? They didn't hold that the President or the Attorney General cannot authorize such a wiretap. They just said that he had to get judicial approval?

Mr. FRIEDMAN. Exactly, but where is that judicial approval other than Title III? Title III narrowed the area in which they could get such judicial approval and Congress established procedures under which that judicial approval might be secured. But if Congress said this is the only place in which you can get such judicial procedure, then the Executive would have to follow that procedure or else they wouldn't get the kind of approval the Supreme Court required them to get.

Mr. KASTENMEIER. Did you wish to continue, Mr. Friedman, or are you open to questions?

Mr. FRIEDMAN. I am open to questions.

Mr. KASTENMEIER. I yield to the gentleman from Massachusetts.

Mr. DRINAN. You make the case well here on page 18 and before that, that it really doesn't matter if we have warrants required for national security cases. But wouldn't you broaden the argument and say that all Federal judges seem unable or unwilling to be very stringent in the issuance of warrants?

And I recall statistics where only an infinitesimal number of requests of any kind for narcotics or organized crime or kidnapping warrants had in fact been denied by Federal judges.

Mr. FRIEDMAN. I think that is true. I mean, the warrant procedure is some protection, more because of the recordkeeping rather than because the judge is really going to say no to the Government. And when the Government comes in with a national security excuse, I take it that the judges are going to be more loath to say no to the Government because they feel the security of the Nation may be at issue.

Mr. DRINAN. No, but can you demonstrate that by statistics? Have they in fact been more lax, if you will, or more loathe to deny the Government in national security cases than they have in the other routine crimes?

Mr. FRIEDMAN. But the Government never comes to them on a national security case. The Government will not come to a judge. As we said earlier, in the testimony, if they cannot go under Title III——

Mr. DRINAN. I know that and that is the very point I want to make. Does it really make any difference?

You make the point on page 18 that the only arguable improvement is, if you get a warrant, there would be better recordkeeping.

Mr. FRIEDMAN. That is right.

Mr. DRINAN. But you wouldn't have fewer warrants? I mean, you wouldn't have fewer taps?

Mr. FRIEDMAN. I don't think so.

Mr. DRINAN. That is right. But doesn't the argument carry all the way that you just have to abolish the whole procedure by which a warrant is available at all?

Mr. FRIEDMAN. Well, that is our starting position.

Mr. DRINAN. But you are trying to have it both ways, you are trying to compromise. You are trying to say, well, maybe we could in fact require that national security cases also get a warrant. But if you face the full implication of your argument that it wouldn't really make any difference, what is the point?

Mr. FRIEDMAN. The only improvement is the recordkeeping improvement.

Mr. DRINAN. You say the recordkeeping has some effect, but does it really? In the long run how many people have ever heard of the recordkeeping in their case and how many cases has the Government concealed it? Is it really any compensation, so to speak, or restitution for the violation of the rights?

Mr. FRIEDMAN. Well, I don't think it is any restitution at all. I mean it is better that you do have some records than that you don't have such records.

Mr. DRINAN. I am not even persuaded of that. What benefit is it to the ordinary tappee?

Mr. FRIEDMAN. Well, he may be able to sue and be able to prove that the tap did take place and get some kind of compensation. We are engaged in such suits right now.

Mr. DRINAN. I know. Is Dr. Halperin the first?

Mr. FRIEDMAN. No, there are about three or four others.

Mr. DRINAN. Has anyone ever recovered?

Mr. FRIEDMAN. They have never come to trial. I think they are all at the discovery stage. There are about half-a-dozen cases that we know of which are still in the discovery stage. And as far as I know, no one has ever collected any money under the civil remedy.

Mr. DRINAN. Are mandatory damages provided in the statute?

Mr. FRIEDMAN. They are under 2520.

Mr. DRINAN. That is right. I yield back my time. Thank you.

Mr. KASTENMEIER. The gentleman from Illinois?

Mr. RAILSBACK. No questions.

Mr. KASTENMEIER. The gentleman from Maine?

Mr. COHEN. There are a number of cases where people have brought suit under a violation of the civil rights act and have recovered damages, aren't there? There is a remedy, and I would think that our lawbooks are amply documented with cases of recovery, aren't they, though not specifically on wiretaps?

Mr. FRIEDMAN. Not on wiretap. The 1968 act provides a specific monetary civil rights monetary conpensation for damages of $100 a day for procurement, use, interception, and use of a tap held to be illegal.

Mr. COHEN. But under prior civil rights acts and suits, aren't there awards for damages?

Mr. FRIEDMAN. There have been awards.

Mr. COHEN. Compensatory and punitive damages as well?

Mr. FRIEDMAN. Right. When police officers break in someone's home without a warrant, there have been civil rights action suits brough and there are cases in which they do pay damages. And so to that extent, as I was saying to Congressman Drinan, the recordkeeping may be useful in establishing the basis of a civil rights suit for

damages. And that is why it is some improvement, but I mean on a scale of 100, I just don't know. A warrant procedure may help somewhat in the invasion of rights that we are talking about.

Mr. COHEN. The only other question I had is, I think you made the statement earlier that if you were going to try to narrow the areas where the Federal Government could wiretap legally by getting warrants you would limit it to foreign spies or agents. Would that be a practicable distinction in your mind? To say that, if one is a foreign agent as opposed to a U.S. citizen engaged in spying on behalf of foreign governments, a tap could be issued. Is that a workable distinction?

Mr. FRIEDMAN. Well, but the point is that title III already specifies that you can get a warrant and you can secure a tap if you are investigating sabotage, espionage, or treason. So if an American citizen is engaging in those activities, or there is a possible investigation into those activities, the Government already has the procedure it needs.

Mr. COHEN. And in your opinion would that be sufficient, would title III be sufficient, for example, on the breaking in of Dr. Fielding's office? Had they sought a title III warrant in that instance, based on espionage activities on behalf of foreign governments, would that be sufficient?

Mr. FRIEDMAN. Well, again I keep——

Mr. COHEN. I am sorry, I came in late and didn't hear all of your testimony.

Mr. FRIEDMAN. No. I just remember Senator Ervin making the same kind of argument when John Ehrlichman was on the stand. And he asked what justification was there, I mean, Lewis Fielding didn't have any secrets, he wasn't a possible spy, so how can you justify breaking into his office? Now I take it that some judge might have asked the same kind of question. And they said "well, we want to wiretap Dr. Fielding's office because one of his patients is Daniel Ellsberg, who we think might have given some information to the Russians."

Now maybe a judge would say: "I just can't buy that. That is ridiculous. You know, if you want to wiretap anyone, wiretap Ellsberg. Why do you want to wiretap his psychiatrist?" And he might say "I am not going to give you a warrant for that."

So hopefully it is just conceivable that some judge might block some of the justifications that have been offered for a national security tap.

But our point is that title III, that if you are concerned about national security, that title III gives you what powers you need, except for some very limited area involving "foreign nationals"; the exact contours of which I still haven't figured out. But we certainly don't need any vague, general or elusive concept such as national security and foreign intelligence and then just say well we will add a warrant to that and that is going to answer the problems. Because it is just not going to answer the problem at all because judges won't say no, generally and because it would simply open up this massive invasion of rights we have been talking about.

Mr. COHEN. In other words, you don't think there would be sufficient insulation through the judicial process, enough of a buffer, notwithstanding any report that might be filed by this committee or any other committee that would spell out for example some of the factors that might be considered? You would still not have that kind of confidence in the judiciary side?

Mr. FRIEDMAN. No. I think if you limit it to a specific kind of objective standard and really veer in on those specific kinds of limits, for foreign intelligence taps, that would be helpful. That is more important than a warrant procedure.

Mr. COHEN. But spelling out that kind of procedure, and giving guidelines to the Judiciary, you wouldn't reject out of hand at least the impartiality and the conscientiousness of a Federal judge in screening these proposals?

Mr. FRIEDMAN. No, I wouldn't. I just don't think you should just lay it in a judge's lap and say "decide on the basis of national security" without defining what national security would be because the judge is at a loss then and judges are as much concerned about the safety of the Nation as anyone. You know, they are willing to lean over backwards to give the Government what it says it needs in order to protect the Nation against foreign attack.

Mr. COHEN. Absent any guidelines from Congress?

Mr. FRIEDMAN. Absent any guidelines. But the guidelines are important. I mean, the guidelines must be laid down with great specificity or else the court is going to turn around and say, well, Congress has said a warrant procedure is OK and so they thereby sanctioned exactly what the Executive has done here and I think that would be a disaster.

Mr. COHEN. You don't dispute the basic fact—and I think you said this in one of your statements—that the Government has an inherent right to protect itself against foreign activities? You don't dispute that basic premise?

Mr. FRIEDMAN. I don't dispute that, but Congress can specify the way in which that power shall be exercised.

Mr. COHEN. OK, that is all I have.

Mr. KASTENMEIER. Just a couple more questions. You are talking mostly about the Justice Department and the Bureau conducting the wiretapping. What about other entities that might be engaged in wiretapping or surveillance other than these, presumably for the purposes of national security? I think it was you or it was your colleague who referred to campaign workers who were I think wiretapped by the U.S. military in Germany in 1972.

Mr. FRIEDMAN. That is correct.

Mr. KASTENMEIER. What were the circumstances there? Why would the U.S. military intelligence be interested in wiretapping these individuals?

Mr. FRIEDMAN. Well, their purported justification—and they have internal memoranda—and their justification memos on down the line, their justification was that they were certain American civilians in Germany were creating dissidence among the troups and were creating dissidence by urging them to vote for McGovern, among other things. And so an elaborate surveillance procedure was estab-

lished by the Army in Germany to wiretap campaign workers for McGovern in Germany, to wiretap people who were working with lawyers' groups defending Army personnel in Germany. And it was institutionalized. The whole unit was set up in effect to do some of this work and a considerable amount of material was developed. And the justification was, well, we didn't want dissidence among our troops in Germany.

Now in addition to that, there was a document just filed last week in Chicago, in the Chicago conspiracy case. The contempt charges in the Chicago conspiracy case are up on appeal in the seventh circuit. And once again, there was a whole request for wiretap information there; a request for wiretaps started as long ago as 1969. And last week the Government admitted that another Government agency had wiretapped some of the defendants in the Chicago case. We don't know what agency it was. It wasn't the Justice Department. It wasn't the FBI. It wasn't the Internal Revenue Service. Some other Government agency had been engaging in wiretapping. Maybe it was the Secret Service, maybe it was some other Army unit, but the Government has admitted in papers filed in the case last week that still another agency engaged in the taps and they just discovered it, you know, within the last month.

Mr. KASTENMEIER. In the case of the campaign workers in Germany, who would initiate that in a situation like that? Would it be someone in Washington or a general in Germany?

Mr. FRIEDMAN. We think it was inspired in the Army high command in Germany. The Army just took it on itself.

Mr. KASTENMEIER. Does it derive the same authority to conduct wiretaps as the Attorney General and the FBI, through this exception for national security purposes?

Where does it derive the authority to do it?

Mr. FRIEDMAN. Well, they never had to justify it to anyone. They never said "we have the authority" because they never had to come to court. Presumably they feel that they are in Germany and the Constitution doesn't apply and therefore they don't have to worry about it. They can do whatever they want. As long as it doesn't violate German law.

Mr. KASTENMEIER. Is that case being challenged?

Mr. FRIEDMAN. Oh, yes. We haven't got the Government's answer in that so we don't know what its justifications are yet.

Mr. KASTENMEIER. With State and local enforcement officers or entities, do you find similar problems? You don't probably find national security problems, but it terms of individuals exposed to or subject to surveillance or wiretapping by authorities without their knowledge, are there any of cases like that at the local or State level?

Mr. FRIEDMAN. There are a number of cases. We have a case in New York against what was called the Bureau of Stratgic Services in the New York City Police and they kept their eye on a number of political organizations, antiwar groups, black groups, allegedly black militant groups, and very recently they admitted that they

had at one time or another conducted surveillance on some 250-odd groups within their jurisdiction.

Now this is not necessarily a wiretap. It is often an informer that is placed in the midst of these groups and reports back to the police.

Mr. KASTENMEIER. Are these activities for which they would need to obtain a warrant?

Mr. FRIEDMAN. Well, for an informer, you don't.

Mr. KASTENMEIER. No. Not just informers, but I am talking about electronic surveillance, wiretapping.

Mr. FRIEDMAN. Sometimes.

Mr. KASTENMEIER. And where is it necessary to obtain a warrant and where do they obtain such a warrant?

Mr. FRIEDMAN. Presumably yes they do. I mean there may be some violent groups. I mean if the California police knew something about the SLA and they wanted to place a tap on a phone that they were using, I assume they could get a warrant without any difficulty, from a judge. But of course again there is a definitional problem. The SLA is not, you know, the Philadelphia Resistance Group or a Quaker group which was in fact surveilled by the FBI in the Vietnam war days. And that is a problem, when criminal investigation gets into political intelligence. And the FBI is very quick to assume that the two are closely related concepts. And if they are justified in doing it in one case, they feel, they are justified in doing it in another case.

Mr. KASTENMEIER. Yes. The gentleman from Massachusetts?

Mr. DRINAN. Some time ago, right after the *Keith* decision in 1972, I went to the GAO and asked them to investigate the number of warrantless taps. They have not been very successful at it. The Department of Justice and the FBI are not talking. But Dr. Halperin in his testimony says that the number has remained the same. And I gather that you would conclude that the number, despite the decision in *Keith*, remains the same. And I assume from the testimony here that Richardson and Ruckelshaus and Saxbe as Attorney Generals have in effect said that the *Keith* decision has no impact. They may change the terminology, but they just go after everything they need, and they just say that this person has some connection with the foreign government.

Mr. FRIEDMAN. Exactly so.

Mr. DRINAN. So it is fair to say the the *Keith* decision, despite the fact that it was 8 to 0, and the people hailed it as a great victory, really in effect means nothing?

Mr. FREIDMAN. Well, it means something.

Mr. DRINAN. I mean, in actual practice.

Mr. FRIEDMAN. In actual practice? That is the problem. I think Dr. Halperin's phone was tapped not on a national security basis but on a foreign intelligence basis and the Government can always convince itself that there is some element of some foreign activity involved in almost any tap that it can put on.

In the Jewish Defense League case they said, well, if the Jewish Defense League harasses Russian diplomats, even though they have no relation, even though the league itself has no relation to a foreign

power, what they do affects our foriegn relations and therefore we can install the tap on the basis of a foreign policy exception.

Mr. DRINAN. Where precisely is the list, is the catalog of all the the warrantless taps that has been started since the *Keith* decision? In the office of the Attorney General, I suppose. But is there somebody lower than that that really knows how many and for what purposes?

Mr. FREIDMAN. Well, the Justice Department is only bound under title III to give a report each year on the number of warrants applied for and warrants secured, but there is no requirement under the statute that they report on the warrantless tap.

Mr. DRINAN. I know that, but where is this list? I assume they must have a list because the Attorney General I assume or his designated authority must have it personally, but the GAO can't find the list.

Mr. FRIEDMAN. Well, when I questioned Mr. Ruckelshaus about this, he said there is a folder, a file of authorizations that is maintained in the office of the Director of the FBI and that contains all authorizations for national security taps. And so therefore the Director or in that case it was the Assistant Director actually had possession of the authorization for the Kissinger taps. There is a file in which that memorandum from the Director to the Attorney General, which is then returned to the Director of the FBI, is maintained and it is a total list of what the taps, are, who was tapped and for what length of time.

Mr. DRINAN. In Dr. Halperin's case, do you people expect to subpena that list?

Mr. FREIDMAN. Well, not the whole list. We expect to subpena the authorization for his particular taps, certainly. But I don't know that we would be entitled to all of the others that may not be related to that case.

Mr. DRINAN. Mr. Chairman, and counsel, I would suggest that this committee certainly would be entitled to see that even if we have to subpena it. I think it would be a fascinating list.

Mr. FRIEDMAN. Well, you know, Attorney General Saxbe said his first week in office, the first thing they did was put three national security tap authorizations in front of him and he signed them. So I mean it is still going on all of the time.

Mr. DRINAN. He said that was just routine, that he wasn't initiating those.

Mr. KASTENMEIER. We have, under my letter of April 11 to the Attorney General, requested detailed information on wiretapping, including warrantless wiretapping, and the Attorney General or the Deputy Attorney General will be here to testify in person and we will have an opportunity to ask him further about that.

Mr. DRINAN. On that point, Mr. Chairman, I read your good letter, and I hope that it is precise and demanding enough so that they can't evade it, but I am inclined to think from my experience with the GAO that they will, and they will either say that it doesn't exist or its exists in different places or that it can't be released.

In any event we will find out I hope when the Department of Justice representative comes.

Thank you sir.

Mr. KASTENMEIER. I just have one other question. So long as you have that much experience, would wiretaps initiated by the White House, and I am not talking now about the Department of Justice or the Bureau, be cataloged by the Attorney General or might they be separately conducted and not accounted for outside of the White House?

Mr. FRIEDMAN. Well, our understanding is that every tap handled by the FBI must be authorized personally by the Attorney General whether it is initiated by the National Security Council or the President or anyone else. It must be funneled to the Attorney General because his signature is necessary on any tap, even under any kind of national security tap. And we believe there is nothing that we know of to the contrary except that there may be other agencies that do it. The Army I don't think got the permission of the Attorney General to conduct its electronic surveillance. We don't know about the Secret Service.

Mr. KASTENMEIER. You did mention, and this intrigues me, that outside of the Treasury Department, the Secret Service, and I don't know about the Central Intelligence Agency, but certainly military organizations and presumably a number of Government entities, Federal Government entities, can be conducting wiretaps which would not be accounted for by the Attorney General. Is that correct?

Mr. FRIEDMAN. I think that is correct. I think that the Treasury Department wiretapping may not go through the Attorney General at all, in which case these authorization documents just don't exist. This was the procedure where the FBI was the installing agency. J. Edgar Hoover wanted a written authorization from the Attorney General before he would authorize.

Mr. KASTENMEIER. And, of course, the reason for my question is a very important one. It is so that this committee can get a feel for the dimension of what is transpiring and how pervasive it is. We want to know who authorizes wiretapping. It would be a little simpler if it were just one entity that authorized everything, but if it is not, the job is more complex it would seem.

Thank you very much, Mr. Friedman, for your most excellent testimony and your help to the committee.

[The statement of John Shattuck, Esq., and Leon Friedman, Esq., follows:]

STATEMEN OF JOHN H. F. SHATTUCK AND LEON FRIEDMAN, NATIONAL STAFF COUNSEL AMERICAN CIVIL LIBERTEES UNION

Our names are John H. F. Shattuck and Leon Friedman and we are staff counsel for the American Civil Liberties Union, a nationwide non-partisan organization of more than 275,000 members devoted to the protection of the Bill of Rights. The ACLU has always been extremely concerned about the invasion of constitutionally protected rights through government installed wiretaps.

We also act as counsel for Morton Halperin in a civil suit for damages based on what we claim was an illegal wiretap of his home telephone in the

so-called Kissinger taps. [*Halperin* v. *Kissinger, et al.*, Civ. 1187-73 (D.D.C.)] As we explain more fully below, Dr. Halperin's home telephone was tapped for 21 months. He had left government employ after the first four months of the tap. We believe that the Kissinger taps of 13 government employees and 4 newsmen illustrate some of the worst features of national security taps and will refer to specific examples throughout our testimony.

I. THE ACLU'S GENERAL OPPOSITION TO WIRETAPPING.

In May 1961, at the outset of the national debate over wiretapping, the National Board of Directors of the American Civil Liberties Union adopted the following resolution:

"The ACLU stands unequivocally against wiretapping or the use of other electronic eavesdropping devices by any person for any reason whatever. It rests its policy on the specific stipulations of the Fourth Amendment against the use of general warrants and searches by government officials, and on the basic right of the citizen to the protection of his privacy [ACLU Board Minutes, May 1, 1961]."

In our view the recent abusive wiretap practices by the federal government—particularly those conducted in the name of "national security"—have underscored and reinforced the soundness of our broad opposition to wiretapping. Before discussing these recent abusive practices and suggesting ways in which they might be brought under legislative control, if they are not to be eliminated altogether as they ought to be, it is necessary to set forth the general considerations on which the ACLU's wiretap policy is based.

A. Wiretapping is an Inherently Unreasonable Search and Seizure.

The principal argument against the constitutionality of any kind of electronic eavesdropping is that it necessarily results in a search and seizure too sweeping to comply with the particularity requirements of the Fourth Amendment. The technology itself stands in the way of any kind of effective control, such as a conventional search warrant "authorizing the seizure of tangible evidence" and particularly describing the things to be seized, as well as giving prior notice to the subject of the search except under exigent circumstances. Cf. *Osborn* v. *United States*, 385 U.S. 323, 329-30 (1966).

The technology of electronic surveillance makes the wiretap search of telephone conversations infinitely more intrusive than the physical search of a home or a person, even when the wiretap is conducted pursuant to a search warrant. The typical federal wiretap in 1972, installed with a warrant, involved the interception of 1,023 conversations among 66 persons over an average period of more than three weeks. These wiretap statistics are reported annually by the Justice Department, and were cited last year by Senator McClellan as the best evidence available of the manner in which wiretapping was being *controlled and restricted* under Title III of the Omnibus Crime Control and Safe Streets Act of 1968. See CONG. REC. S 7934 (April 30, 1973) (remarks of Senator McClellan). Such statistics, however, demonstrate the opposite: when a tap is placed on a telephone the eavesdropper inevitably hears all the conversations of everyone who talks on that line, whether the subject calls from the tapped number, to that number, or is called by someone using that phone, and no matter how irrevelant or privileged the communication.

Electronic surveillance, therefore, is the prime example of Justice Brandeis' foreboding in *Olmstead* v. *United States*, 277 U.S. 438, 473 (1928) that "discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet." Even where circumscribed within the confines of Title III, wiretapping represents an intensive and extensive invasion of private speech and thought with almost no parallel. Wiretap devices intrude so deeply and so grossly, they discourage people from speaking freely, and, as Justice Brennan has warned, if such devices proliferate widely, we may find ourselves in a society where the only sure way to guard one's privacy "is to keep one's mouth shut on all occasions." *Lopez* v. *United States*, 373 U.S. 427, 450 (1963).

B. The "Restrictions" Imposed by Title III Merely Under-Score the Constitutional Objections to Wiretapping.

The attempts made by Congress to impose restrictions on wiretapping through the warrant procedure authorized by Title III illustrate the inherent overbreadth of a wiretapping search. See generally Schwertz, *The Legitimation of Electronic Eavesdropping: The Politics of Law and Order*, 67 MICH. L. REV. 455 (1969).

First, Title III authorizes continuous eavesdropping for potentially unlimited periods of time. Section 2518(5) permits a wiretap to be installed for an initial period of thirty days with an unlimited number of thirty-day extensions upon renewed showings of probable cause. Similarly, sections 2518(1)(d) and (4)(e) permit uninterrupted surveillance over a "period of time," and do not require the eavesdropper to limit his interception to specific conversations. Although several lower federal courts have followed the lead of the Supreme Court in *Berger* v. *New York*, 388 U.S. 71 (1967), and require "minimization" of the interceptions to conversations of the subject, see, e.g., *United States* v. *King*, 335 F. Supp. 523 (C.D., Cal. 1971), the impracticality of this requirement is reflected by the vagueness of the statute."

Second, particularizing the items to be seized—a condition required by the Fourth Amendment—means little in the context of a wiretap "seizure" of all conversations which occur during the period of the tap. For this reason, Title III is limited to a vague requirement that the "type of communication sought to be intercepted" be described in the warrant application. Since section 2517(5) of the Act permits a court to ratify retroactively the seizure of *any* conversations overheard on a tap authorized by the statute, the search is not necessarily limited to the type of communication described in the warrant. This ignores the Fourth Amendment principle prohibiting "seizure of one thing under a warrant describing another." *Marron* v. *United States*, 275 U.S. 192, 196 (1927), but it is simply a recognition of what is inevitable in the "special circumstances" of wiretapping.

Third, nothing in Title III prohibits the interception of privileged communications. Again, the sheer impracticality of minimizing or screening intercepted conversations often overcomes a basic consideration of the Fourth Amendment which is reflected in virtually every search and seizure context except wiretapping. It is hardly surprising, therefore, that wiretapping more than any other search technique has become a "widespread" method of penetrating the attorney-client privilege. See, e.g., *United States* v. *Roberts*, 389 U.S. 18 (1967); *Berger* v. *New York*, 388 U.S. 41 (1967); see *infra*, Section II. F .3.

Fourth, there are substantial indications that the surveillance apparatus authorized by Title III is not used as much for gathering criminal evidence as it is for collecting general intelligence. These indications are evident in the statistics of the relatively few convictions obtained through evidence secured by wiretaps, [see Schwartz *Report on the Costs and Benefits of Electronic Surveillance* (ACLU, 1973)]. The indications are overwhelming, moreover with respect to "national security" wiretapping, to which we will address the remainder of our statement. Because intelligence gathering necessarily lacks particularity, and is often aimed at 'preventive surveillance' and speech in general, its accomplishment by a technique fraught with constitutional difficulties further underscores our broad objection to wiretapping. The requirements of the Fourth Amendment are most strict when the object of a search is protected by the First Amendment. *Stanford* v. *Texas*, 379 U.S. 476 (1965). When wiretaps are used to seize speech under a generalized claim of "national security intelligence gathering" our constitutional objections to the practice are greatest.

II. NATIONAL SECURITY WIRETAPPING

The invasion of constitutional rights through the installation and use of national security wiretaps is even worse than it is with respect to Title III taps. The following outline of the general procedures applicable to national security taps, with special emphasis on the Kissinger taps, shows what these problems are.

A. Vague and Inadequate Justifications

In order to initiate the procedures for installing a national security tap, an official must prepare a written justification as to why the tap is necessary. This proposed justification is then sent to the FBI which will administer the tap. The Director of the FBI in turn requests an authorization from the Attorney General to install the tap.

But these justifications can be and have been extremely thin. Former Acting FBI Director William Ruckelshaus testified last summer, for example, that full reasons for justification were often not given for taps installed at the request of the National Security Council:

Mr. RUCKELSHAUS. However, having been a Director of the FBI for 75 days, I know that general procedure in the FBI was that, where a given national security wiretap was originated by information the FBI had, there was a very elaborate request made of the Attorney General justifying his authorization for a given tap, but where the FBI received a request from the National Security Council, this elaboration was not, as a rule, made.

Senator CASE. Could that elaborate procedure be avoided by having a Director get Henry Kissinger to say "Let me have the dope?"

Mr. RUCKELSHAUS. Sure.

Senator CASE. In other words, the authorizing document does not necessarily, in itself, tell the full story.

Mr. RUCKELSHAUS. That's possible. [Hearings before the Committee on Foreign Relations, U.S. Senate, on Nomination of Henry Kissinger to be Secretary of State, 93d Cong., 1st Sess., at p. 284].

In other instances, the reasons given for a particular tap could be so general that no judge would accept them if a request were made for a warrant. But because the justification memorandum is an internal document between or within the Justice Department and the FBI, no one could challenge the assertions made. One egregious example was the "national security" tap placed on the telephone of Martin Luther King, Jr. According to Victor Navasky's excellent account in *Kennedy Justice* (Athenaeum 1971), the FBI sought to put a tap on Dr. King's phone because they claimed that two of his close friends and associates may have been Communists. (These charges were never proved and would have been irrelevant even if they were true.) Taps were placed on Dr. King's home phone, his office phone in Atlanta and another office phone in New York. If the FBI were really concerned about possible influence of Dr. King by his allegedly Communist friends, they should have put the tap on them, not on King. Navasky quotes an "old hand at Justice" to this effect: "If you really want to find out about A's attempt to influence B, you tap A not B." (Id., at pp. 149–50).

In the case of the Kissinger taps, two of the seventeen persons tapped allegedly had no access to the national security information whatever. [*New York Times*, October 15, 1973]. Yet such access was the stated reason for each of the taps.

In another recent series of national security wiretaps, the United States Army sought to justify tapping the telephones of American civilians in West Germany on the ground that they were responsible for "dissidence" among American troops. The principal targets were a group of civilian lawyers in Heidelberg and Americans in Berlin who supported Senator George McGovern in the 1972 Presidential campaign. No action was ever taken against either group, and the Army has since conceded that its wiretapping and other surveillance activities in Germany were "excessive." The American civilians have filed a civil suit for damages, claiming that the taps were illegal. *Berlin Democratic Club, et al.* v. *Schlesinger, et al.*, Civil Action No. 310–74 (D.D.C.).

B. Evasion of Title III

Another aspect of national security taps which has emerged from several recent civil cases is the fact that the government consistently avoids using the provisions of Title III when it can assert any basis for a national security tap. Thus even if the government could secure a Title III warrant because a specific crime enumerated in 18 U.S.C. Section 2516 is under investigation, it will not do so if it can offer some excuse for claiming that national security is involved and no warrant is necessary.

One recent example involved the Jewish Defense League. In connection with an investigation into the physical attacks on Soviet diplomats during demonstrations in New York City by the J.D.L., the FBI installed a wiretap on the asserted basis of the government's foreign intelligence activities. It plainly could have proceeded under Title III, however, since possible violation of 18 U.S.C. Section 2101 was involved. See *Zweibon* v. *Mitchell*, _____ F. Supp. _____ (D.D.C. 1973).

In a number of other cases the government could have obtained a warrant under Title III, but relied instead on a national security rationale. E.g., *United States* v. *Ayres*, No. 48104 (E.D. Mich. 1973) (alleged SDS bombing conspiracy). In many such cases, the wiretaps were found to be illegal because of the lack of a warrant. See *United States* v. *Ahmad*, 335 F. Supp. 1198 (M.D. Penn. 1971) (no finding of purpose to gather foreign intelligence; fruits to be supressed; defendants entitled to post-trial adversary hearing on taint); *United States* v. *Joffe*, 71 Cr. 480 (E.D.N.Y., June 18, 1971) (tap directed at defendants or their premises; turnover ordered); *United States* v. *United States District Court*, 407 U.S. 297 (1972); *United States* v. *Hoffman*, 334 F. Supp. 504 (D.D.C. 1971); *United States v. Smith*, 321 F. Supp. 424 (C.D.Cal. 1971) (domestic security surveillances).

As we discuss below, the government could obtain a warrant under Title III even when foreign intelligence gathering is involved. Section 2516 specifically includes the investigation of espionage and sabotage as a basis for a Title III warrant. Thus there is no need for a foreign intelligence exception to warrant requirements in this area. See *United States* v. *Butenko*, 318 F. Supp. 66 (D.N.J. 1970).

C. Lack of Procedural Safeguards

The effect of using a national security tap instead of proceeding under Title III is to eliminate what few, though inadequate, procedural safeguards exist to protect citizens from the "dread of subjection to an unchecked surveillance power." *United States* v. *United States District Court*, 407 U.S. 297, 314 (1972). First, no application is made to a neutral and detached magistrate to issue a warrant. Second, no limitation is placed on the period of time for which the interception is to be maintained. Title III expressly requires a court order to specify the time period for which the wiretap is authorized. 18 U.S.C. 2518(1)(d) and (4)(e). Court ordered wiretaps which were unlimited in duration have been held to be illegal. "We observe that the absence of a date on the order made its duration unlimited by its own terms. As such, it apparently authorized a wiretap for an unreasonable length of time which rendered it invalid." *United States* v. *Lamoge*, 458 F. 2d 197, 199 (6th Cir., 1972).

Third, in national security taps no attempt is made to minimize invasion of the privacy of the persons using a wiretapped phone. With respect to court ordered taps, however, 18 U.S.C. §2518(5) so provides. This requirement of minimization has been held to invalidate court ordered wiretaps when no effort was made to screen out innocent calls. In *United States* v. *King*, 335 F. Supp. 523 (C.D. Cal. 1971) the district court suppressed all telephone calls intercepted by court order on a suspected narcotics dealer. The government agents had intercepted and recorded all telephone conversations, although 60% did not relate to the purpose of the wiretap. Similarly, in *United States* v. *Scott*, 331 F. Supp. 233 (D.D.C., 1971), the Court condemned the wiretaps in question because the surveillance included overhears of family conversations totally unrelated to the purpose of the wiretaps:

"If the court were to allow the government agents to indiscriminately intercept every conversation made and to continue monioring such calls when it became clear that they were not related to the "authorized objectives" of the wiretap and in violation of the limiting provisions of the order, such order would become meaningless verbiage and the protections of the right of privacy outlined in *Berger* and *Katz* would be illusory. 331 F. Supp. at 248."

Fourth, §2518(8)(a) requires that recordings of all wiretaps installed by court order "shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years." The Second Circuit recently suggested that this provision of Title III should apply to national security wiretaps as well as those installed by court order. In *United States* v. *Huss*, 482 F.2d 38 (2nd Cir., 1973), the court said:

"The government urges us to adopt the principle that considerations which bear on judicially authorized wiretaps are not applicable to the wiretaps under discussion, because so-called warrantless domestic security bugging not expressly held unlawful at the time these taps were installed, was not found to be invalid until the Supreme Court decided the question in *United States* v. *United States District Court*, 407 U.S. 297 (1972). We are urged to hold therefore, that the warehousing provision, 18 U.S.C. Sec 2518(8)(a) which requires preservation of records only for electronic surveillance authorized by Title III . . . does not apply to the wiretaps here under review. Since we do not today announce a per se rule that the government's failure to preserve the wiretap tapes must result in a reversal of these contempt orders, we need not decide the question. We note, however, that it would be a startling, if not preposterous ruling that permits a more relaxed standard for illegal than for legal wiretaps. Such a precept would serve only to encourage illegal wiretapping. Every order . . . shall contain a provision that the authorization to intercept . . . shall be conducted in such a way as to minimize the interception of such communication not otherwise subject to interception." [482 F.2d at 48].

D. The Halperin Tap as an Illustration of All the Infirmities of Current National Security Wiretap Practices.

The public evidence produced to date in the civil litigation arising out of the twenty-one month wiretap on the home telephone of Dr. Morton Halperin, *Halperin* v. *Kissinger, et al.*, Civil Action No. 1187–73 (D.D.C.), illustrates in detail each of the foregoing infirmities in existing national security wiretap practices:[1]

1. The government has conceded that there was only a single authorization existed for the wiretaps in question (Answer, par. 17). Thus the original authorization either had no time limit or it authorized the wiretap for the entire 21 month period that it was in force—a highly unlikely possibility. Under either alternative, the wiretap violated existing strictures on the establishment of a set term for electronic surveillance. The New York wiretap statute held unconstitutional in *Berger* v. *New York*, 388 U.S. 41 (1967) permitted wiretaps for 2 month periods after a single showing of probable cause. The Court condemned this practice as a sweeping invasion of Fourth Amendment rights [388 U.S. at 59].

2. The government has admitted that it intercepted, recorded and transcribed every telephone conversation over the Halperins' home telephone for the entire 21-month period, including conversations of the three minor plaintiffs (aged 7, 9 and 11), personal and family conversations, as well as political and professional conversations of Dr. Halperin. These are all totally unrelated to the supposed leak of national security information. The government, therefore, clearly exceeded the minimization requirements applicable to Title III wiretaps.

3. The government has conceded that the original tapes of the Halperins' wiretap telephone were erased after the logs were transcribed. Such an erasure is contrary to the procedural requirements establishd for court ordered wiretaps by Title III, 18 U.S.C. §2518(8)(a).

4. The government and John Mitchell both admitted in the Halperin case that the procedure for renewal every 90 days of a national security tap was not followed: "no other authorization was either sought or procured by any of the federal defendants." (Government's Answer, par. 17). Thus instead of seven separate authoritarians every 90 days over the 21-month period of the tap which should have been obtained under normal operating procedures, the government secured only one authorization which the Attorney General at the time does not recall signing.

What emerges from this brief outline is that national security taps lead to a massive invasion of a citizen's constitutional rights. Because the taps do not have a limit imposed by the court, they often continue for months and even years. In the Halperin case, the tap continued on his home phone for

---

[1] Additional documentary evidence has recently been produced by the government in the suit pursuant to plaintiffs' motion to compel discovery, which was granted by the District Court on April 1, 1974. Plaintiffs' and their counsel, however, are currently bound by a Protective Order not to disclose these documents except by further order of the Court.

21 months, the last 17 of which he was not in government employ. According to statistics introduced by Senator Edward Kennedy, the average national security tap in 1970 was installed for a minimum of 71 days to a maximum of 200 days. This was 3 to 9 times greater than the average length of a Title III wiretap. [*Warrantless Wiretapping*, Hearings before the Subcommittee on Administrative Practice and Procedure, Senate Committee on the Judiciary, 92nd Cong., 2d Sess., June 29, 1972, at p. 70].

Because there is no statutory requiremest of minimization, every phone conversation may be overheard with no effort made to screen out innocent calls.

Because there is no requirement of preserving the taps, there is no way to check on whether the transcriptions or summaries of the taps were accurate.

E. Inadequate Recordkeeping and the Breakdown of Accountability.

Apart from the documentary support required for the authorization of a national security wiretap, there are recordkeeping requirements which must be followed by the Justice Department with respect to any wiretap. The principal requirement is that the names of all persons who are overheard on a wiretap must be entered on the FBI's "Elsur Index," a central indexing system kept both for internal investigatory purposes and for the purpose of preparing responses to wiretap discovery orders. See Deposition of former Acting FBI Director William D. Ruckelshaus, July 25, 1973, at p. 12, *Halperin* v. *Kissinger, et al. supra.*

Wiretap litigation in recent years, however, has revealed that these recordkeeping requirements are so loosely followed that the government routinely evades or fails to disclose the full extent of its wiretap activity with respect to particular litigants. In national security cases the temptation appears to be particularly great for the government simply not to enter the names of wiretap subjects on the "Elsur Index." This is what happened in the Halperin case, and there is reason to believe it was also true with respect to the other so-called "Kissinger taps."

The good faith recordkeeping of the government is placed in serious doubt when, after repeated denials in courts of any electronic surveillance, it suddenly about-faces and admits that private litigants were overheard on a national security tap. See, e.g., *Philadelphia Resistance* v. *Mitchell*, 58 F.R.D. 139 (E.D., Pa. 1973) (Amended Answer to Complaint ¶25A), *United States* v. *Russo-Ellsburg*, No. 9393 (C.D., Cal. 1973); *United States* v. *Smilow*, 472 F.2d 1193, 1195 (2d Cir., 1972); *Kinoy* v. *Mitchell*, 70 Civ. 5698 RJW (S.D.N.Y.); *Dellinger* v. *Mitchell*, Civ. Action No. 1768–69 (D.D.C.) (Transcript of Hearing on Discovery Motions, November 7, 1973, pp. 32–33). The government's original answer to the complaint in *Philadelphia Resistance*, for example, denied that any surveillance of the plaintiff had occurred. Seven months later, it filed an amended answer in which it admitted overhearing plaintiffs' conversations during the course of electronic surveillance of others. In the Ellsburg prosecution the government finally admitted its surveillance of Ellsburg after a year of repeated denials. Upon an order by Judge Byrne to produce all records concerning the taps, the government claimed these records had been "lost" (*New York Times*, May 11, 1973). As is now well known, however, a few days after the dismissal of the case, Robert Mardian, the former head of the Internal Security Division of the Justice Department, revealed that the missing records were in fact in a White House safe (*New York Times*, May 15, 1973).

Three years after commencement of a civil suit for damages for illegal electronic surveillance in *Kinvoy* v. *Mitchell, supra*, the government disclosed that there had been 23 incidental overhearings of the plaintiff in national security taps over a 15-year period, despite an initial statement to the contrary. Another instance of government inability or unwillingness to discover the existence of electronic surveillance was recently disclosed in *Dellinger* v. *Mitchell, supra*. After more than four years of denying that one of the plaintiffs had ever been overheard, during the argument on plaintiffs' motion for discovery, the government finally admitted over hearing him (Transcript, at 32–33). The Second Circuit in *United States* v. *Smilow*, 472 F.2d 1193, 1195 (2d Cir., 1972), summed up as follows the courts' increasing concern at the

government's inability to discover and admit its wiretapping activities in a prosecution of a grand jury witness for contempt of court:

"We cannot forbear expressing our regret that those representing the Government in court were unable, until such a late date, to discover the true state of affairs with regard to official wiretapping of the defendant's telephone conversations * * * We trust that in the future the Government will be more thorough in the investigation of such matters."

One explanation for the government's remarkable inability to keep track of its own surveillance activity must be that its recordkeeping system is woefully inadequate. This system has enabled the government to avoid full compliance with any wiretap discovery order, since apparently it cannot determine from its records the identities of all persons overheard in any given instance. An example of this problem occurred in *United States* v. *Smilow*, *supra*, where the government lawyers claimed they had not been able to discover that a person named "Jeffrey" had been overheard because he introduced himself in the intercepted conversation as "Jeff." The Court of Appeals, however, observed tartly that "it does not require much imagination to anticipate that an individual named Jeffrey might be known as Jeff to friends or acquaintances" [472 F.2d at 1195].

A particularly shocking illustration of the inadequacy the government's recordkeeping system was revealed in *United States* v. *Ayers*, No. 48104 (E.D., Mich.), a conspiracy prosecution of the Weathermen faction of S.D.S. Pursuant to an interim court order to disclose any transcripts of the defendants' intercepted conversations the government inadvertently turned over twelve days of logs of all conversations overhead on one domestic security tap. The logs noted 500 overhearings, half of which were listed as "unidentified." Upon inspection, the defendants were able to determine that a number of these overhearings were of the defendants themselves and of their attorneys. In each of those instances, the relevant transcripts had not been turned over to the defendants, presumably because the government had not realized that they represented conversations of the defendants. *United States v. Ayers*, *supra*. (Supplemental Affidavit in Support of Defendants' Motion for Discovery, pp. 2–3, October 1973). The government ultimately dropped the prosecution so that it would not have to disclose the full scope of the wiretappings.

A series of deliberate and "patently unbelievable" misrepresentations by the government which "strained common sense" and culminated in the unexplained destruction of illegal wiretap tapes on the eve of compelled disclosure, led the Court of Appeals for the Second Circuit in *United States* v. *Huss*, 482 F.2d 38 (2d Cir. 1973), to dismiss contempt charges against an informer who had refused to testify before the grand jury. The court refused to accept as true the governmnt's "good faith" representation that the destroyed tapes would not have revealed matters of importance:

"[i]ndeed, the government's good faith did not prevent illegal wiretapping here, nor did the government's good faith prevent it from search illegally or from narrating an account of that search which the Court found to be incredible [482 F.2d at 50]."

Characterizing the attitude of the government as "cavalier, carefree and careless," the Court observed that the wiretap recordkeeping had made a "mockery of the labors of Congress to tailor [Title III] with precision" and had "offend[ed] the spirit of liberty which has distinguished this nation from its birth" [Id. at 52].

Because of these inadequate and deceptive recordkeeping practices, courts are increasingly skeptical about the conclusory and ambiguous affidavits denying electronic surveillance which are regularly submitted by the government in response to court orders to disclose. *In re Korman*, 13 CrL 2310 (7th Cir., June 8, 1973); *United States* v. *Alter*, 482 F. 2d 1016, 1027 (9th Cir., 1973); *In re Horn*, 458 F.2d 468, 471 (3rd Cir., 1972); *Beverly* v. *United States*, 468 F. 2d 732, 745 (5th Cir., 1972). The Seventh Circuit, for example, recently refused to accept a general letter from a government attorney denying electronic surveillance, which was submitted to counter the allegation of a grand jury witness that his interrogation was based on the fruits of an illegal wiretap. *In re Korman*, *supra*. Although the Court stated that it had previously been willing to accept such general denials as sufficient, "certain

indiscretions" had come to its attention which "seem to militate for a more formal and binding denial than those which were [previously] found to be adequate." *Id.*

The Ninth Circuit has similarly refused to accept such generalized denials of wiretapping. *United States* v. *Alter*, *supra*. The denial affidavit in *Alter* simply stated who the affidavit was, that he had "caused an official inquiry to be made with the appropriate Federal agencies," which were listed, and that based on the results of the inquiry there had been no electronic surveillance of the defendant. The court criticized such a conclusory statement because: "1. it supplied no information whatever about the identity of the stated no facts from which the court could conclude that the six listed either the substance of his inquires or the substance of the replies, 3. it stated no facts from which the court could conclude that the six listed agencies were the only governmental agencies which could have been involved in electronic surveillance, and 4. it did not reveal the dates of claimed surveillance to which the inquiries were addressed."

The court concluded by pointing out that "[i]f any of the conclusions in the affidavit were later proved wrong, it would be virtually impossible to establish that the affidavit was perjured" [482 F.2d at 1027].

In summary, the lack of recordkeeping standards in national security wiretaps allows the government to be most cavalier in what records it keeps and how much it discloses about its activities. As a result, it can hide the facts as to who it wiretaps (as it did initially in the Kissinger taps), or at the least be very careless in disclosing what it has done. This lack of accountability seriously compounds all the other problems relating to national security taps which we have discussed.

F. Invasion of Constitutional Rights

National security taps necessarily lead to a massive intrusion into Constitutionally protected rights.

1. *First Amendment Rights.*—National security taps have repeatedly invaded First Amendment rights to political association and free speech. In the Halperin case, for example, Dr. Halperin became a consultant to Senator Muskie's presidential campaign in 1970 and 1971. All his conversations in this area were intercepted and presumably made available to persons in the White House who were extremely interestd in Snator Muskie's ideas and efforts at this time. The government has also admitted that it monitored Dr. Halperin's efforts to write critical articles of government activities after he left the governmen.

Published reports indicate that a second target of the Kissinger taps also worked for Senator Muskie and was tapped during the very time he was an active campaign worker.

In the J.D.L. case, many persons who actively supported the J.D.L. and called its office with pledges of money or assistance had their names recorded for the use by the government. Any attempt to obtain these names directly would have been denied under the authority of the Supreme Court's decision in *NAACP* v. *Alabama*. 357 .S. 449 (1958).

There have been numerous other cases where dissident groups or civil rights activists or opponents of the Vietnam War, were wiretapped under constitutionally baseless circumstances. We have already alluded to the wiretap of Martin Luther King, Jr., who was tapped because some associates allegedly had Communist ties. In a notorious memorandum produced before the Senate Watergate Committee, Egil Krogh and David Young reported to John Ehrlichman that Richard Barnet and Marc Raskin of the Institute for Policy Studies, highly vocal opponents of the Nixon Administration's Vietnam policies, were "overheard." (Ervin Committee hearings, p. 2644.) We also know that David Dellinger and other defendants in the Chicago Conspiracy trial were overheard numerous times during the period when they were planning and carrying out protest rallies against government policy.

2. *Fourth Amendment Rights.*—The sweeping intrusion into a person's right to privacy by a wiretap has already been set forth above. Everything that is said on a tapped telephone is swept up by the government's electronic machinery. In the Halperin case, every conversation on the plaintiff's home telephone was recorded and transcribed over a 21-month period. These in-

cluded family conversations between husband and wife or parents and children, conversations between the minor children and their friends as well as the political discussions mentioned above. These conversations were carefully transcribed by an anonymous government clerks, summarized by FBI agents and sent regularly to White House officials, who then knew virtually everything about the Halperin's thoughts and activities for nearly two years. All this was done in the name of protecting national security and it was done for seventeen months after Dr. Halperin had left government employ.

As Mr. Justice Powell pointed out in his opinion for a unanimous Court in *United States* v. *United States District Court*, 407 U.S. at *313*, the historic relationship between the First and Fourth Amendments is dramatically evident in the context of a national security wiretap, and it is particularly evident in a tap like the Halperins':

"National security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. "Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power." *Marcus* v. *Search Warrant*, 367 U.S. 717, 724 (1961)."

3. *Sixth Amendment Rights.*—The sweeping nature of a wiretap necessarily means that many privileged communications will be overheard by government eavesdroppers. In recent years there have been numerous instances of lawyer-client calls being overheard. In the days before Title III, bugs or taps were in police headquarters—almost certainly an intrusion upon lawyer-client conversations. See Schwartz, op. cit. 478–79.

Overhearings of lawyer-client conversations have often occurred in national security cases. See. e.g., *Kinoy* v. *Mitchell*, *supra* (defense lawyer overheard 23 times). In a brief submitted to the Seventh Circuit Court of Appeals in the Dellinger contempt case last week, for example, the following assertions were made about FBI wiretapping of the defendants and their lawyers in the Chicago conspiracy case:

"(i) Despite Mr. Mitchell's memorandum to Mr. Hoover, dated July 14, 1969, directing that FBI agents avoid monitoring defendants and their attorneys during the conspiracy trial, a memorandum heavily relied upon by the government in this case, they in fact did so and had to be reminded of the directive by the central office of the FBI.

"(ii) FBI agents were specifically directed to frame even their *internal* reports to the FBI so as to conceal the source of their material, the result of which is that records in FBI files will not reveal what FBI agents know.

"(iii) The FBI was continuously making personality assessments of the defendants in the Chicago conspiracy trial, which obviously were a key to what may well have been the structuring of trial court proceedings so as to develop reactions by the defendants.

"(iv) As a foundation for a claim of a foreign security exception, the FBI has directed its agents to submit "excised" logs which would reveal only the recordings of converastions showing foreign involvement; thus, logs submitted *in camera* to a court on a claim that surveillance was for foreign security purposes are not an accurate report of the true logs. *In re Dellinger*, 73–2017, Reply brief for Appellants pp. 20a–21."

These assertions were based upon government documents produced in a civil case pending in the District of Columbia, *Dellinger* v. *Mitchell*, Civ. No. 1768–69.

Another recent instance of a national security wiretap interferring with Sixth Amendment rights is the Army's surveillance of civilian American attorneys in West Germany. Conversations among lawyers working for the Lawyers' Military Defense Committee (a plaintiff in *Berlin Democratic Club, et al.* v. *Schlesinger, et al., supra*) and their clients were intercepted on at least one wiretap installed on the phone of an American free lance journalist and consultant to LMDC. Conversations overheard on the wiretap, as revealed by Army documents summarizing them, included discussions about how to conduct the court martial defense of Larry Johnson a black GI who has since been discharged from the Army. According to the Army intelligence agents who disclosed the wiretapping, more than fifteen volumes of classified surveillance

documents, including the records of other wiretaps on LMDC lawyers, were destroyed by the Army immediately after the disclosures occurred last August, thus further indicating that the Army knew the entire operation was illegal.[3]

III. CURBING NATIONAL SECURITY ABUSES

It has been suggested that the answer to the abuses noted above is to require a separable warrant procedure apart from Title III for all national security or foreign intelligence wiretaps. We do not believe that such a procedure standing alone would adequately deal with the problems we have been discussing.

A. Definition of National Security

In the first place the definition of national security is so elusive that a separate warrant procedure is not likely to restrict the wide range of wiretaps that have been installed in the past. 'National security" was used to justify many aspects of the Watergate cover-up. It was used to justify the wiretap of Martin Luther King, Jr. It was used to justify the break-in of the office of Dr. Lewis Fielding, Daniel Ellsberg's psychiatrist. It was used to justify the wiretap of Morton Halperin for 17 months after he left the government.

The difficulty of defining "national security" was eloquently expressed by Egil Krogh, Jr., soon after he pleaded guilty to his part in the Ellsberg break-in:

"While I early concluded that the operation had been a mistake, it is only recently that I have come to regard it as unlawful. I see now that the key is the effect that the term "national security" had on my judgment. The very words served to block critical analysis. It seemed at least presumptuous if not unpatriotic to inquire into just what the significance of national security was.

"When the issue was the proper response to a demonstration, for example, it was natural for me to question whether the proposed course was not excessive. The relative rankings of the rights of demonstrators and the protection of law and order could be debated, and the range of possible accommodations explored, without the subjects' of patriotism and loyalty even rising to the level of consciousness. But to suggest that national security was being improperly invoked was to invite a confrontation with patriotism and loyalty and so appeared to be beyond the scope and in contravention of the faithful performance of the duties of my office.

"Yet what is national security? I mentioned that all of the potential uses of the information sought in the Fielding incident were consistent with my then concept of national security. The discrediting of Dr. Ellsberg, which today strikes me as repulsive and an inconceivable national security goal, at the time would have appeared a means of blocking the possibility that he would become such a popular figure that others possessed of classified information would be encouraged to emulate him. More broadly, it would serve to diminish any influence he might have in mobilizing opposition to the course of ending the Vietnam war that had been set by the President. And that course was the very definition of national security. Freedom of the President to pursue his planned course was the ultimate national security objective. [*New York Times*, January 25, 1974, p. 161"

"Foreign intelligence" is equally difficult to define. A recent law review article succinctly points out the problem:

---

[3] It should be noted that the Army dropped its charges against Spec. 4 John McDougal, one of the Army intelligence agents who made the "unauthorized disclosures", after McDougal's lawyer gave notice that he intended to base his defense on the illegality and unconstitutionality of the surveillance. An even more telling admission by the Army that its surveillance program could not be defended in court was the rescission of Eighth Army Regulation 381-25 ("Military Intelligence, Counterdissidence Program") in early August 1973, immediately after the first reports about the wiretapping began to appear in the press, and little more than a week after the Regulation was promulgated on July 23. The Regulation defined "dissidence" as "manifestation of a rejection of military, political or social standards," and authorized military intelligence agents to collect information about civilian or military "dissidence" by a variety of covert means.

"The definition of a foreign security surveillance is far from clear. Almost any problem of governmental concern could be said to relate, at least remotely, to the national security, and to bear, at least potentially, on the country's relations with foreign powers. If loosely drawn, a foreign security exception to the warrant requirement could thus be very broad. *United States District Court* did not narrow its potential scope, having been decided as a purely domestic case, and lower court cases which have applied the foreign security exception have done so quite expansively. In *Zweibon* v. *Mitchell*, for example, the court accepted as grounds for the warrantless surveillance of the Jewish Defense League the possibility that that group's anti-Soviet protest activities might bring adverse reaction from the Government of the Soviet Union and harm to American citizens in that country. The case suggests that individuals may be the subject of warrantless foreign security surveillance without themselves having the least affinity with a foreign power, if their activities threaten to affect the behavior of foreign powers. (footnotes omitted) Note, 87 Harv. L. Rev. 976, 977–78 (1974)"

In one current case, in which we are representing an Arab-American activist lawyer in a civil suit for wiretap damages, an asesrted national security justification by the government for barring discovery was rejected by the District Court. The government had submitted an *ex parte* affidavit which undoubtedly was more detailed than its own internal justification memoranda. *Jabara* v. *Kelley*, 42 LW 2528 (E.D. Mich. March 21, 1974).

In the so-called Kissinger taps, the justification offered for wiretapping 13 government employees and 4 newsmen was that there was a leak of national security information to the press. The government asserted a "foreign affairs"/"national security" rationale for the tap on the Halperin home by the facile logic that because intelligence organizations read American newspapers, any leak of information to the newspapers is tantamount to a spy covertly conveying information to a foreign government.* This rationale would expose to unwarranted executive wiretapping all the hundreds of thousands of government and private industry employees who have access to classified information, all former employees who had such access, all members of Congress, and all newsmen who are potential recipients of such information.

B. Ex Parte Application for a Warrant

The fact that a judge would have to pass on the government's application for a tap is not likely to solve the problem. The government could offer a plausible excuse why a national security tap was necessary. Under the *ex parte* circumstances of the application, it is unlikely that a judge would dispute the *government's contentions* as to why the tap should be installed.

In the Halperin case, for example, the government has argued as follows.

"The early months of 1969 were particularly sensitive times with regard to the formulation of this country's foreign policies and the establishment of our future relations with other nations. *Statement by the President*, 9 Presidential Documents 694 (1973). During this period, policies were being considered which would establish this country's fundamental approach to major foreign policy issues such as the Strategic Arms Limitation Talks (SALT), Vietnam and many other national security issues. *Ibid.* Because of the sensitive nature of these matters, the secrecy of each was of vital importance, and placed in lawyers' offices or in other places where attorneys would speak to their clients. The Detroit police allegedly wiretapped every public telephone the success or failure of each program turned in many instances upon the maintenance of the necessary security. *Ibid.* However, notwithstanding the critical need for such security during this period, the Government was confronted with leaks to the press of documents which were considered of the greatest importance to the national security . . . . access to the classified information which had been disclosed to the press was limited to a few officials and employees within the Government, Dr. Henry A. Kissinger, then Special Assistant to the President, was directed by the President to provide the

---

*The government's argument was as follows: ". . . the electronic surveillance of [Dr. Halperin's home telephone] was conducted by the Executive for foreign policy purposes and for the protection of national security information against foreign intelligence activities."

Federal Bureau of Investigation with the names of certain individuals who had such access. *Hearing on Nomination of Henry A. Kissinger, supra* at 12. One of the names provided to the Federal Bureau of Investigation by Dr. Kissinger's office was that of Dr. Morton H. Halperin, then a member of the National Security Council staff.

"However, notwithstanding this and other investigations being conducted by the Federal Bureau of Investigation and additional governmental efforts to curb the unauthorized disclosure of classified information, press leaks involving the most sensitive of foreign policy matters continued through 1969, 1970 and 1971, and the surveillance of Dr. Halperin was thus continued throughout this period until its termination on February 10, 1971."

The plaintiffs' were able to dispute the government's argument, however, and obtain discovery in the case, despite the assertions of national security. But without an adversary hearing, the government's assertions might well have been accepted by the court.

A warrant procedure would add limited protection if the concept of national security remains as broad and is as frequently asserted as it is now. In our view, therefore, the principal task facing the Congress is the enactment of broad prohibitory legislation. This legislation should be backed up by a warrant procedure only with respect to the extremely narrow area in which any wiretapping at all is permitted.

C. Inadequate Protection of Constitutional Rights

The only arguable improvement that would come out of a separate warrant procedure for broadly defined national security/foreign intelligence taps would be better recordkeeping. The Title III requirements of a warrant and the housekeeping provisions of Section 2518 would mean that the government would not be able to be so careless in accounting for the existence of a tap. But other Constitutional infirmities mentioned above would still exist.

The government would still be able to wiretap its political enemies under the pretext o national security and thereby inhibit the exercise of their First Amendment rights. The invasion of Fourth Amendment rights would be as sweeping as they are now, as would Sixth Amendment infringements. A warrant procedure would not overcome these constitutional objections.

D. Warrant Procedures and Recordkeeping Requirements

It has been argued that there must be some procedure for the government to secure foreign intelligence information through a wiretap to protect the national defense or safety; and that the government must have some means to protect itself against foreign espionage. It must be allowed to obtain intelligence to meet clear and present external dangers before they ripen into direct violence against the nation.

It has been argued that there must be some procedure for the government already has specific authority to wiretap, the constitutionality of which has not yet been decided. The crimes outlined in Section 2516 which justify a wiretap under Title III include espionage, sabotage, treason, rioting, and similar crimes. As the Supreme Court pointed out in *United States* v. *United States District Court*, 407 U.S. at 321. "Judges may be counted upon to be especially conscious of security requirements in national security cases. Title III . . . already has imposed this responsibility on the judiciary in connection with such crimes as espionage, sabotage, and treason. §2516(1)(a)(c)."

With respect to domestic activities which are under investigation by the Government for "national security" reasons, the Supreme Court has already spoken. Where "there is on evidence of any involvement, directly or indirectly of a foreign power," the Fourth Amendment applies. *United States* v. *United States District Court*, 470 U.S. at 309.

The Justice Department in its Congressional testimony has conceded that the Supreme Court's decision narrows the area of possible executive discretion to wiretap in foreign intelligence situations. These must be limited to circumstances where "such factors [exist] as substantial financing, control by or active collaboration with a foreign government or agencies thereof in unlawful activities directed against the government of the United States." Furthermore the Justice Department has conceded that "such factors will be present in a very minimum number of situations." Testimony of Deputy Assistant Attorney General Kevin T. Maroney, *Hearings, Warrantless Wiretapping supra*, p. 12.

We must point out that the Government's position in each national security wiretap case cited in our testimony is at variance with this concession.

Title III leaves open the question of discretion for Executive action in the area of foreign intelligence gathering or to protect national security information against foreign intelligence activities. This area of discretion as to which the Congress has taken no position and which the Supreme Court narrowed in the *Keith* case, is still too broad. At a minimum the limits of foreign intelligence wiretapping should begin with the definitions offered above. But in drawing up these definitions we hope that Congress does not authorize what it is seeking to prohibit.

We believe that a warrant procedure for foreign intelligence wiretaps does not go far enough. It does not meet the definitional problems mentioned above. It may be interpreted as lending Congressional sanction to an unconstitutional practice. The need for accountability is great and any exercise of executive discretion in this area should be subject to legislative definition and subsequent judicial review.

However if Congress does not affirmatively prohibit these kinds of wiretaps, a warrant procedure under strict definitions and standards is a conceivable alternative. As we noted above, a warrant requirement would lead to some kind of Executive accountability. It would mean that the courts could initially check on the government's claim of foreign security and later hold it to account if it exceeded its authority. It would mean that the targets of illegal use of this power might obtain redress, and Congress could also determine whether its standards have been met.

CONCLUSION

The right of privacy is perhaps the most important right of American citizens. A wiretap is and has been a most serious invasion of that right. A warrant requirement in order to legitimate vague national security wiretap practices will not cure these incursions upon the Constitution.

Thank you for this opportunity to appear before the Subcommittee today.

Mr. KASTENMEIER. The hour is late and I would like to offer the Chair's apologies to Dr. Morton Halperin, who has patiently waited to testify.

Dr. Halperin holds his Ph.D. in political science and served the Government both as Deputy Assistant Secretary of Defense during the Johnson administration and as an assistant to Henry Kissinger at the National Security Council during the early part of this administration.

Dr. Halperin was the subject of a warrantless national security wiretap for over 1½ years after leaving the Government.

We welcome you and you may proceed any way you wish.

TESTIMONY OF MORTON HALPERIN, PH. D., FORMER NATIONAL SECURITY COUNCIL STAFFER

Dr. HALPERIN. Mr. Chairman, it is a great privilege for me to appear before this committee. I propose to discuss warrantless wiretapping rationalized by the incantation "national security."

Depending on one's perspective this can be said to be a subject on which I am biased, or it can be said to be one on which I speak from great experience. In any case, my involvement with warrantless wiretaps is, which unvoluntary, quite extensive. For 21 months, the words of members of my family and those who called us on the telephone or used the telephone themselves, were duly summarized and copies of these summaries were sent to high administration officials, including Henry Kissinger and H. R. Haldeman. During

all but the first 4 of these 21 months, I was a private citizen with no access to classified information, but with an active involvement in public affairs.

The lawsuit brought by my family has been brought against those we believe responsible for this surveillance and has now progressed to the stage where we have been given copies of the summaries of these telephone conversations and other documents. And I have spent, I might say, most of the last week reading these documents and they are both fascinating and frightening. I am prohibited by the court's order from discussing this material. And in restraint and the fact that Mr. Freidman and Mr. Shattuck have discussed what we know about the case from other materials. I propose to focus my remarks on some more general questions about my case in so far as I am able to do so.

My remarks then will be focused on three questions: (1) What is the current practice of the Justice Department; (2) what are the benefits of such surveillance; and (3) what should be done.

The starting point for any inquiry about current practice is of of course the *Keith* decision. I find Justice Powell's decision in that case unambiguous, totally unambiguous. As I read it, he says that, electronic surveillance of an American citizen requires a warrant under the procedures of the omnibus crime bill unless he or she is an "agent" of a foreign power. And the Court of course, reached no judgment at all about whether a warrant would be required for the surveillance of foreign powers or their agents. But it defined "agents" as those having a significant connection with a foreign power. Therefore, in my view, its practice under *Keith* should be straightforward, as Mr. Freedman suggests, and clearly it is not.

Warrants should be required under title 3 unless the surveillance is of a foreign power or its agents, and agents is narrowly defined. Now the Justice Department witnesses who testified before the Senate Judiciary Committee shortly after the *Keith* decision gave precisely this interpretation. William Ruckleshaus, when he was Acting Director of the FBI and later Deputy Attorney General, also gave this interpretation of the decision. But as already suggested, other signs are more disquieting.

The number of warrantless surveillances does not appear to have gone down. Mr. Richardson has presented the opinion that the *Keith* case did not cover any surveillance in any way related to foreign policy—the Jewish Defense League was attacking an embassy or in my case because of the view that foreign powers read newspapers and therefore anything that involves anything that might get into a newspaper, the Justice Department explicitly says involves the activities of a "foreign power."

Therefore, there is great uncertainty about what the current practices are of the Justice Department and very disquieting indications that in fact very little has been accomplished by *Keith*. After all, the *Keith* case itself involved the CIA, the blowing up of a CIA installation so presumably that would now be said to be involved with a foreign power.

In my view the committee should discover very precisely what the current practices are and insist that, if there is to be any war-

rantless surveillance, until there is any further legislation, that it be limited to foreign powers, and their "agents" narrowly defined as those who have a significant connection with a foreign power, but in cases where espionage is not involved.

Because if espionage is involved, then a warrant should be required under title 3.

Let me turn now to the question of the value of warrantless surveillance for national security purposes. In my judgment, such surveillance has extremely limited value and can in no sense be called vital to the security of the United States. I should make it clear that on that specific question of what one learns from such surveillance, my information is only negative. Never during my 3 or 4 or more years in the Defense Department and the White House did I read a report which I knew to be based on electronic surveillance conducted in the United States, although I routinely saw material from far more sensitive sources.

Occasionally and at random, one might pick up a useful piece of information from an electronic surveillance of an embassy, but the systematic take must, as regards the activities of foreign powers, be mere gossip. Such things as whether the Foreign Minister is coming over this week or next week and whether he plans to stop in New York for 2 or 3 days.

As George Kennan makes clear in his memoirs, every foreign service officer going abroad assumes that his office and home phones are tapped. Nothing is said by a diplomat on a phone unless he is prepared or even in some cases desires that what he says is to be overheard by the host government.

Now not only is electronic surveillance unlikely to yield significant information, but also the American Government has many other sources of information of significantly greater value.

This is, of course, a very difficult subject to discuss in a public session or even in executive session of a Congressional committee limited to Top Secret information. I may simply assert that the executive Branch has many sources of information on the activities of foreign governments, that no single one of these sources can be considered "vital" although many yield information of far greater value than could conceivably come from electronic surveillance.

I would urge this committee to demand from the executive branch a very careful "all source" evaluation of the absolute and relative value of information obtained from warrantless electronic surveillance for national security purposes.

Now if I am right that surveillance has relatively little value, you may wonder why it is carried on so extensively and so vigorously defended by the Justice Department and the FBI. The explanation in my view lies in large part in the way the American executive bureaucracy functions.

Let me try to suggest just a few key points involved there:

First, involving the struggle over missions. One of the most enduring characteristics of the Federal bureaucracies is the struggle over responsibilities. Each agency has a view of its essence, its core activity, and struggles to keep responsibility for the areas it has while broadening into other related areas.

Such a struggle over turf engages the FBI in its relations with the CIA, NSA, DIA, and the Armed Services Intelligence branches. The FBI seeks exclusive control over investigations within the United States while the foreign intelligence agencies seek responsibility for gathering all national security information.

When such a conflict exists, the agency responsible for the mission must constantly demonstrate its willingness and ability to perform that mission.

The competing organizations seek to show that the agency is either unwilling or unable to commit the resources necessary to do the job right. And in this classic situation, the consuming agencies continue to raise their demands while the performing group struggles to meet the requests.

The foreign intelligence agencies, eager for the responsibility to monitor embassies, would like nothing better than a record of FBI refusals to perform a requested surveillance.

The FBI is unwilling to create such a record. Thus, requests for surveillance are generated whenever they are remotely plausible, and the FBI is reluctant to challenge the asserted need.

Second, is what I call, the extravagant use of "free goods"; whenever something is free to an agency, it is likely to ask for a great deal of it.

The budgetary and manpower costs of the surveillance are not charged to the foreign policy agencies. If on the other hand, the NSA for example, wanted to increase its monitoring of coded messages to and from country *X*, it would have to find the money and personnel to do so. But telephone taps or bugs of embassies are "free goods", paid for from the FBI budget. Bureaucracies, like individuals, have a tendency to consume a great deal of any free good without asking how much it is costing someone else.

Third, the failure to take other values into account. Bureaucracies feel neither the responsibility nor the capability to take the values of society, other than those with which they are formally charged, into account in making decisions. For the foreign affairs agencies, who generate the requests for surveillance, not only is there no budgetary cost, but the possible infringement of constitutional rights is not viewed as a legitimate concern. Their responsibility is to gather information needed by foreign policy decisionmakers; it is somebody else's job to worry about civil liberties.

One might expect the attorney general to play this role, but he is simply not equipped to do so unless he has a staff involved in this process which can challenge national security surveillance on the grounds that it interferes with people's civil liberties and of course he has no such staff.

Finally, there is the unplanned payoffs of value to the bureaucracy. Often, an agency will pursue a program with enthusiasm for reasons unrelated to why it is asked to undertake the activity. I suspect such a phenomenon is as work here.

There is little doubt that the FBI has an insatiable appetite for information about domestic groups and individuals with an interest in one or another foreign country. Taps on embassy phones yield much information about who gets into contact with foreign govern-

ments and why. From the point of view of the FBI itself, the most valuable aspect of embassy taps may very well be the leads that it provides to American citizens who are of interest to the Bureau.

If this last phenomenon explains at least in part why our surveillance is so extensive despite the meager returns for national security, it also explains what is wrong with such surveillance. Taps on embassies do not merely pick up the conversations of diplomats talking to each other. They allow the FBI to listen in on the conversations of American citizens discussing their political beliefs. These citizens have no way of knowing which phones to avoid and do not learn that their conversations have been overheard unless and until they are indicted for a criminal offense.

Let me conclude by stating briefly what I believe should be done by way of legislation.

Let me state clearly that my own preference would be to abolish all wiretapping. I believe it is an unwarranted intrusion of the privacy of American citizens. And I do not believe that it is either legal under the Fourth Amendment or even that, if it is, that it is good policy to permit such taps.

But assuming that the Congress is not prepared to take the steps of abolishing such wiretaps, then it seems to me that it should urgently consider some most modest steps:

First, I think warrants should be required for all surveillance of American citizens and resident aliens and should be issued under the procedures of the Omnibus Crime bill in situations where there is probable cause to believe that a crime has been committed.

And I think given the Justice Department's interpretation of *Keith*, this requires legislation.

As far as taps on embassy personnel and nonresident aliens and noncitizens, who may be agents of foreign powers, again my preference would be that all such surveillance be made illegal and that section 3, which permits such an exception, be removed from the legislation. But again, if Congress is not prepared to take that step of banning embassy taps, but under the lesser standard of reason to believe that information of importance to the national security will be learned.

And I do not believe that information obtained from such taps should be usable in a court of law. My view of the main purpose of requiring warrants on embassy taps is that if your permit any area in which taps can be conducted without a warrant, no matter how narrowly you define that area, say it can only be on embassies or ambassadors, the Government will always extend the area. They will say "well we are tapping A because Ambassador Jones frequently visits him or it is his mistress' house" or whatever. I think the only way to make it clear that, if you conduct a tap without a warrant, you are doing something illegal is to require a warrant on every tap, whether it is on an embassy or ambassador or an American citizen.

Finally I think, as far as the telephone companies, that legislation should provide that the telephone company is to assist in placing taps on phones only when it is given a copy of a warrant and maintains a copy of that warrant in its files. In my view the behavior of

the phone company has been even more reprehensible than that of the Government because the phone company is after all a contractee of an individual and one really doesn't have any choice but to go to the C&P Telephone Co. if one lives in Maryland and one wants a telephone. There is not much competition in this area.

And the phone company, which I let into my home in order to get its phone service, permitted the FBI, without a warrant, without any justification being given to the phone company, without even a piece of paper being given to them, permitted them—and not only permitted but put a tap on my phone and gave the end of the wire to the FBI in order to listen into conversations.

I believe that the phone company should be put on notice that its behavior is criminal if it permits a tap without a warrant.

That is another reason why I believe warrants have to be required for all taps. I believe the telephone company should be told very explicitly that a wiretap without a warrant is illegal and I believe this is of great importance because my understanding is that a tap with the help of the telephone company can be put on in 10 minutes. It is easy to put on a tap with the help of the telephone company but a tap without the support and assistance of the telephone company is difficult to put on and it is relatively easy to detect.

Mr. Chairman, that I think concludes my remarks except to say that the changes that I think should be made, if in fact taps are not to be banned entirely, are consistent with the bill that the Chairman has introduced and I am pleased to indicate my support for it.

Mr. KASTENMEIER. I am pleased to have your support for it, Dr. Halperin. You have talked about wiretapping and to some extent electronic surveillance. Do you feel there are other ways the Government, through mere following of citizens or shadowing of them, engages in pursuits which invade the privacy of its citizens?

Mr. HALPERIN. I am sure that these things go on. In the public materials in my lawsuit there is no reference to any surveillance of me other than the phone taps but there is of course a great deal of information on the record of the Government doing this in other cases, of attending meetings, of taking down the names of people there, of taking pictures of meetings and so on.

Mr. KASTENMEIER. How did you happen to discover that you were being wiretapped?

If you are able to say, was this an accidental discovery?

Mr. HALPERIN. No, Daniel Ellsberg happened to be in my home on one occasion and made a phone call and that fact was revealed at the criminal trial where he had been indicted for conduct involved with the Pentagon Papers.

Mr. KASTENMEIER. I see.

Mr. HALPERIN. And the Government revealed there that he had been overheard on surveillance, not of him, but of me.

Mr. KASTENMEIER. Do you have any questions? We might have time for a question. Otherwise we are again being called to the floor for a vote.

Mr. DRINAN. No. I have a few but I can talk to Dr. Halperin afterwards. I am interested in pages 7 and 8 of his testimony, but

I don't want to hold him. I want to apologize because he stayed all day here and we appreciate it.

I want to tell him his testimony has been extraordinarily helpful.

Mr. KASTENMEIER. Yes, the committee is indeed indebted to you for your appearance today and for your statement. It is a brief statement but it is a very useful one and we appreciate your appearance.

Thank you very much. Dr. Halperin.

[The statement of Dr. Halperin follows:]

TESTIMONY OF MORTON H. HALPERIN, PH.D., FORMER NATIONAL SECURITY COUNCIL STAFFER

It is a great privilege for me to appear before this committee. I propose to discuss warrantless wiretapping rationalized by the incantation "national security."

Depending on one's perspective this can be said to be a subject on which I am biased, or it can be said to be one on which I speak from great experience. In any case, my involvement with warrantless wiretaps is extensive. For 21 months, with the aid of the C&P Telephone Company, agents of the FBI recorded and listened to all of the conversations on my home telephone. The words of my family and those who called us or used our phone were duly summarized and copies sent to high administration officials, including Henry Kissinger and H. R. Haldeman. During all but the first four of these 21 months, I was a private citizen with no access to classified information, but in an active involvement in public affairs.

The lawsuit brought by my family against those we believe responsible for this surveillance has progressed to the stage where we have been given copies of the summaries of these telephone conversations and other documents. I am prohibited by the Court's order from discussing this material. In view of this restraint and the fact that, as I understand it, Mr. Friedman will be discussing my suit, as well as others, with you, I propose to focus my remarks on more general questions. I would, of course, be happy to respond to questions about my own case in so far as I am able to do so.

My remarks, focusing on warrantless so-called national security taps, will deal with three questions: (1) what is the current practice of the Justice Department, (2) what are the benefits of such surveillance, and (3) what should be done.

The starting point for any inquiry into current practice is, of course, the *Keith* decision (*U.S.* v. *U.S. District Court* 407 U.S. 297 (1972)). I find Justice Powell's opinion for the Court unambiguous. It says, as I read it, that electronic surveillance of an American citizen requires a warrant under the procedures of the Omnibus Crime Bill unless he or she is an "agent" of a foreign power. The Court reached no judgment as to whether a warrant was required for the surveillance of foreign powers or their "agents," but it defined "'agents" as those having a significant connection with a foreign power.

Practice under *Keith* should be straightforward. Warrants should be required unless the surveillance is of foreign power or its agents, narrowly defined. The Justice Department witness who testified before the Senate Judiciary Committee shortly after the *Keith* decision came down gave this interpretation of its meaning, and William Ruckelshaus took this view when he was Acting Director of the FBI and Deputy Attorney General. Other signs are more disquieting. The number of warrantless surveillances does not appear to have declined significantly since *Keith*. Only six were removed immediately folowing the decision and Elliot Richardson recently testified before two subcommittees of the Senate Judiciary Committee that while he was Attorney General there were an average of approximately 100 warrantless surveillances at any given time. Moreover, in Mr. Richardson's view, *Keith* did not affect any surveillance in any way related to foreign policy. The Justice Department has taken the same position in defending individuals in civil litigation, particularly in the *Zweibon case* (where the position has been upheld by the District Court, *Zweibon* v. *Mitchell* 363 F. Supp. 936 (D.D.C. 1973)) and in *Halperin* v. *Kissinger*.

Thus there is great uncertainty about current practice and disquieting indications that warrantless surveillance continues against American citizens where foreign policy is in one way or another involved. I would urge this committee to urgently seek from the Justice Department a clarification of current practices. The committee should, in my view, insist that if there is to be any warrantless surveillance, pending any further action by Congress on the Court, it should be limited to foreign powers and to their "agents" in the rare case where there is reason to believe that a significant connection exists but where espionage is not suspected.

Let me turn now to the question of the value of warrantless surveillance for national security purposes. In my judgment, such surveillance has extremely limited value and can in no sense be considered vital to the security of the United States. I should make it clear that, on the specific question of what one learns from such surveillance, my information is only negative. Never during my three or more years in the Defense Department and the White House did I read a report which I knew to be based on electronic surveillance in the United States, although I routinely saw material from far more sensitive sources. Occasionally and at random, one might of course pick up a useful piece of information from an electronic surveillance of an embassy, but the systematic take must, as regards the activities of foreign powers, be mere gossip.

As George Kinnan makes clear in his *Memoirs*, for example, every foreign service officer going abroad assumes that his office and home phones are tapped. Nothing is said by the diplomats unless they are prepared, or even want, to have it overheard.

Not only is electronic surveillance unlikely to yield significant information, but also the American government has many other sources of information of significantly greater value. This is, of course, a very difficult subject to discuss in a public session or even in an executive session limited to Top Secret information. Let me simply assert that the executive branch has many sources of information on the activities of foreign governments. No single source is itself "vital," although many yield information of far more value than can conceivably come from electronic surveillance. I would urge this committee to demand from the executive branch a careful "all source" evaluation of the absolute and relative value of information obtained from warrantless electronic surveillance for national security purposes.

If I am right that such surveillance has relatively little value, you may wonder why it is carried on so extensively and so vigorously defended by the Justice Department and the FBI. The explanation lies in large part in the way the bureaucracy of the executive branch functions. Let me just touch on a few key points.

The struggle over missions. One of the most enduring characteristics of the federal bureaucracies is the struggle over responsibilities. Each agency has a view of its essence—its core activity—and struggles to keep responsibility for the areas it has while broadening into other related areas. Such a struggle over turf engages the FBI in its relations with the CIA, NSA, DIA, and the armed services intelligence branches. The FBI seeks exclusive control over investigations within the United States while the "foreign" intelligence agencies seek responsibility for gathering all "national security" information.

When such a conflict exists, the agency responsible for the mission must constantly demonstrate its willingness and ability to perform the mission. The competing organizations seek to show that that agency is unwilling or unable to commit the resources necessary to do the job right. In this classic situation, the consuming agencies continue to raise their demands while the performing group struggles to meet the requests. The foreign intelligence agencies, eager for the responsibility to monitor embassies, would like nothing better than a record of FBI refusals to perform a requested surveillance. The FBI is unwilling to create such a record. Thus requests for surveillance will be generated whenever a remotely plausible case can be made and the FBI will be reluctant to challenge the asserted need.

The extravagant use of "Free Goods." There is another reason why the foreign affairs agencies are likely to be casual about requesting surveillance in the United States. The budgetary and manpower costs of the surveillance is not

charged to them. If NSA wants to increase its monitoring of coded messages to and from country X, it must find the money and trained personnel in its budget. Telephone taps or bugs of the embassy are a "free good," paid for from the FBI budget. Bureaucracies, like individuals, have a tendency to consume a great deal of any free good without asking how much it is costing someone else.

The failure to take other values into account. Bureaucracies feel neither the need nor the capability to take the values of society, other than those with which they are formally charged, into account in making decisions. For the foreign affairs agencies, who generate the requests for surveillance, not only is there no budgetary cost, but the possible infringement of constitutional rights is not viewed as a legitimate concern. Their responsibility is to gather information needed by foreign policy decision makers; it is someone else's job to worry about civil liberties.

One might have expected the Attorney General to play this role, but he has not really been equipped to do so. What he would need is a staff that is skeptical about the foreign policy value of such surveillance and concerned with civil liberties which could make the case against any proposed surveillance. In the absence of such a staff he is likely to be overwhelmed by assertions of what the "national security" indeed requires.

Unplanned payoffs of Value to the Bureaucracy. Often an agency will pursue a program with enthusiasm for reasons unrelated to why it is asked to undertake the activity. I suspect such a phenomenon is at work here.

There is little doubt that the FBI has an insatiable appetite for information about domestic groups and individuals with an interest in one or another foreign country. Taps on embassy phones yield much information about who gets into contact with foreign governments and why. From the point of view of the FBI itself, the most valuable aspect of embassy taps might very well be the leads that they provide to American citizens who are of interest to the Bureau.

If this last phenomenon explains at least in part why such surveillance is so extensive despite the meager returns for national security, it also explains what is wrong with such surveillance. Taps on embassies do not merely pick up the conversations of diplomats talking to each other. They allow the FBI to listen in on the conversations of American citizens discussing their political beliefs. These citizens have no way of knowing which phones to avoid and do not learn that their conversations have been overheard unless and until they are indicted for a criminal offense.

Let me conclude by stating briefly what I believe should be done by way of legislation.

Warrants should be required for all surveillance of American citizens (and resident aliens) and should be issued under the procedures of the Omnibus Crime Bill in situations where there is probable cause to believe that a crime has been committed.

Warrants should also be required for surveillance of embassies and embassy personnel, but under the lesser standard of reason to believe that information of importance to the national security will be learned. I believe that warrants should be required for such taps, among other reasons, so that there can be no ambiguity about the legality of warrantless taps. If some taps, with no one knowing how narrowly circumscribed, are legal without a warrant, officials would always be able to claim that they believed a particular tap was in the limited, permissible category. Only if all electronic surveillance requires a warrant can we have any hope of preventing illegal surveillance.

The telephone company should be instructed to assist as requested in telephone taps when it is given a copy of a warrant, and its assistance in a warrantless tap should be made a crime.

Evidence obtained from an embassy surveillance should not be usable in a criminal prosecution.

These proposals are consistent with H.R. 13825 and I am delighted to endorse that bill.

Mr. KASTENMEIER. This will conclude today's hearings, and on Friday morning next in this room at 10 a.m., the hearings will continue, at which time we will hear from a representative of the Justice Department, the Hon. David O. Cooke, Deputy Assistant Secretary of

Defense and William Camming, attorney for American Telephone and Telegraph Co.

We will ask him a couple of questions which perhaps Mr. Halperin might like to know in connection with the phone company, in connection with some of their practices. Until that time, the subcommittee stands adjourned.

[Whereupon, at 4 p.m., the subcommittee recessed, to reconvene at 10 a.m., Friday, April 26, 1974.]

WIRETAPPING AND ELECTRONIC SURVEILLANCE

FRIDAY, APRIL 26, 1974

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES,
AND THE ADMINISTRATION OF JUSTICE OF THE
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The subcommittee met at 10:10 a.m., pursuant to recess, in room 2141, Rayburn House Office Building, Hon. Robert W. Kastenmeier (chairman) presiding.

Present: Representatives Kastenmeier, Danielson, Drinan, and Smith.

Also present: Bruce A. Lehman, Counsel, and Thomas E. Mooney, Associate Counsel.

Mr. KASTENMEIER. The subcommitte will come to order this morning for the second day of hearings concerning the wiretapping and electronic surveillance.

I would like to announce this morning that Mr. Smith, the gentleman from New York, informs me that there are a group of young people here from Ontario, Canada, and we welcome our Canadian friends to this Subcommittee meeting of the Congress.

Our first witness this morning is the Assistant Attorney General in charge of the Criminal Division, representing the Department of Justice, Mr. Henry Petersen. Mr. Petersen's long and faithful service in the Department of Justice is well known to this committee and we are very pleased to welcome Mr. Petersen. And with Mr. Petersen, I understand, is his Deputy, Mr. Kevin T. Maroney. Gentlemen, you are both welcome.

The Chair will observe, Mr. Petersen, that you have a 35-page statement. And we will accept that for the record. You may not necessarily want to read every line of your statement. If you could summarize, particularly those portions dealing with the legislation it would be helpful. If the Chair may observe, I think at this point the committee is more interested in the policies and practices of the Department than in receiving testimony on legislation, although some of the legislative proposals themselves are original and they appear to be plausible in terms of addressing themselves to the problems involved.

Mr. Petersen, you are most welcome and you may proceed.

TESTIMONY OF HON. HENRY E. PETERSEN, ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE, ACCOMPANIED BY KEVIN T. MARONEY AND PHILIP WHITE

Mr. PETERSEN. Thank you.

I was disposed to read it and on your admonition I thought first of summarizing. I do not really think I can do an effective job of summarizing a 35-page statement.

Mr. PETERSEN. Let me be very brief.

We oppose the bills. That is it.

Now, I think with good reason. First of all, let us start with title III. I think that title III, or what we call title III, the provisions which both prohibit and permit wiretapping are effective safeguards. We have set up an elaborate system. Indeed, many say much too elaborate a system under title III to ensure that the wiretapping procedure in implementation of our criminal investigative function is carefully and wisely utilized. Under our practice over the past 5 years, from 1969, and I do not have a precise figure, I would say not more than 10, and I may be exaggerating, not more than 10 of our applications authorizing attorneys to go to the court have been turned down for lack of probable cause. There is a disagreement between the court and our evaluation of the procedure.

Mr. KASTENMEIER. If I my interrupt, I think probably the figure is less than that. Indeed I was struck with the few turn-downs of requests at both the State and Federal levels. For example, according to the Administrative Office of the U.S. Courts, for the period June 20, 1968, to December 31, 1972, the total number of applications for authority to wiretap was 2,751. The total number of authorizations was 2,744. There were only six denials and one withdrawal. So, your "not more than 10" figure is not far from correct.

Mr. PETERSEN. It reflects a great deal of concern and I am sure some of our agents and some of our lawyers at times consider it to be an excess of redtape, but it requires a procedure that initiates with the lawyer or investigator and involves a close working relationship between the two to develop the probable cause and a formulation of the evidence in affidavit form, and an extensive review procedure in the Organized Crime Section in the Criminal Division, and ultimately with the Attorney General. And we exercise a large degree of discretion. We are conscious of the instances where privileged communications may be intercepted, and we are conscious of the duration of the taps on the statutes authorized 30 days. It is our usual custom to authorize only for 15, and if necessary, to apply for a continuation or a renewal, which again has to be submitted with all of the formulation or reasons on up to the Attorney General. We think the practice has been a salutary one, and we think that it has paid off.

We would not like to see it changed. The statute is complex. It has given rise to a large degree of litigation, particularly with respect to the issue of the so-called Mitchell signatures. You are undoubtedly aware that we take the position that the control that the statute mandates at the policymaking level was, in fact, exer-

cised by the Attorney General, notwithstanding the fact that he did not actually put his signature on each and every one. That issue is under consideration by the Supreme Court and, hopefully, we will have a ruling before the end of the term.

Mr. KASTENMEIER. On that question, has the practice changed because of the challenge?

Mr. PETERSEN. Yes it has. The Attorney General now, as a matter of practice, signs every one unless he is unavailable and then under a specific delegation to me, and another Assistant Attorney General on a standby basis we have the authority to approve in an emergency. And that emergency ought to be distinguished from the emergency provisions of the statute. We exercise our authority only when the Attorney General is unavailable. The emergency provisions of the statute have never been actually utilized, and only in one instance was the emergency provision invoked, and that just very recently in connection with some ongoing extortion scheme where the lives of alleged hostages were threatened. And it was on a weekend and we authorized the Bureau, with the concurrence, telephone concurrence of the Attorney General, to proceed without formal submission of the affidavits and papers. Fortunately, the law enforcement authorities raided the premises where the hostages were alleged to have been held, and there were indeed no hostages and so, we have never had to utilize that emergency authorization. Had it been protracted we would have applied again, I think it is a classic example of the discretion that is employed in the Department of Justice and how carefully, and in a limited fashion, we are exercising those powers that have been granted to us by the Congress.

Perhaps a more controversial issue involves the issue of electronic surveillance in the area of internal security. The phrase, itself, is ambiguous. In the *Keith* case, recently decided, it made the distinction between foreign intelligence and foreign relations matters and domestic security matters, and, obviously, we have followed that case and do not authorize warrantless electronic surveillance in domestic security matters. And the procedure in foreign intelligence and foreign relations matters is now more stringent. The applications are walked over by Bureau agents to the office of the Attorney General. They are hand-delivered from the Attorney General's office and they are brought down to me for my recommendation, and if for any reason I am unavailable Mr. Maroney sees them. They are than hand-carried back with our recommendation to the Attorney General, who personally approves, and approval is done under the specific authority of the President and has been sanctioned by history and custom, at least going back as far as President Roosevelt. The standards we use have recently been supported by the Third Circuit en banc decision in the Ivanov case, and basically those standards are reasonable suspicion and need.

The applications themselves are directed to intelligence and counterintelligence, espionage activities and activities relating to development of intelligence information for assistance to the President in the conduct of foreign relations of the United States.

Whether or not it would ultimately be practical to require submission of those applications to the court is, I suppose, to some

degree an open question. We, in the Department of Justice, think it is rather impractical, if only because it requires a large degree of background in intelligence and the information that constitutes the intelligence to make an informed judgment with respect to whether or not the suspicion is realistic. Whether or not there is a need involves dissemination of a great deal of confidential, secret and top secret information. We think that that is best left to the executive branch and, for that reason, we would oppose a warrant requirement and we think that we are rather firmly supported in that by the *Ivanov* decision.

We have thought about other things in terms of this complex, so-called English system, which I cannot speak of in a wholly authritative fashion, but I am told that they over there have a commission which serves this purpose. In any event, there are people who devote their careers to this sort of thing, and a counterpart proposal here would be to establish a commission with one member appointed by the Congress, one by the Executive and perhaps from the intelligence community.

Mr. SMITH. Mr. Petersen, excuse me just a minute. You are talking now about internal security matters?

Mr. PETERSEN. We are talking about, yes, if that phrase means foreign intelligence, foreign intelligence espionage, counterespionage activities, yes.

Mr. KASTENMEIER. My understanding is you are talking about all warrantless wire taps?

Mr. PETERSEN. Yes, sir.

Mr. KASTENMEIER. Electronic surveillance which involves either internal security or foreign intelligence?

Mr. PETERSEN. That is correct.

Mr. SMITH. This is as opposed to internal problems like organized crime and so forth?

Mr. PETERSEN. That is correct, which are covered by the warrant procedure and which we support and would like to suggest that the Congress not change.

I think that the critical area is in this area of internal security and I think that is where, frankly, I think we need some help. We welcome help from the Congress. We do not want to shoulder this responsibility wholly ourselves. We do not want to say it is not for you. We think it is too important a responsibility and our problem is not to exclude you, but our problem is to bring you in in such a fashion that we are not abdicating Executive functions, that we are not violating the separation of powers, that we are not thrusting our responsibility on you. But, we are performing our obligation in such a fashion that we can recognize, with some degree of confidence, what we are doing and that it is done properly, and the judgments are properly exercised, and that there is not calculated abuse, you know, which we do not condone, but there can be mistakes, and there is a possibility of mistakes.

Mr. SMITH. Mr. Petersen, you were talking about the British system, where there was a commission. It is my understanding that you are saying, in effect, that the commission members had a background in internal security and counterespionage work, so that they

knew the sort of background that you imply is necessary to make an informed judgment?

Mr. PETERSEN. Yes, that is true. But, I do not mean to import parochialism into that concept. I do not mean to suggest that no one from without the intelligence community should be appointed. Indeed, I would think to the contrary, that we would like some fresh thinking in there.

Mr. SMITH. But you would think that there should be some experts on that?

Mr. PETERSEN. That is right. But, there are people who could rapidly develop this factual development and insight into the foreign relations and intelligence problems so far as they affect a major power in the world, so that we could function in that fashion.

The other alternative, which we told to the chairman before, we have no objection to the oversight committee. But we do think, at least I think from my position in the Department of Justice, that an oversight committee by the House or an oversight committee by the Senate is really not the answer. Frankly, there is too much jealously between the bodies or maybe a lack of confidence. I do not know what you call it, but at least there is, one can discern from without the legislative branch, a certain degree of jealousy with respect to what committee even within the House or the Senate does this or that. So, we would like to suggest if that is going to be done it be a joint committee. And I would think it would be advisable, too, that it not be of such broad range that its impact is dissipated. I would like to think that perhaps we could have an oversight committee with respect to internal security problems, or internal security problems as they relate to surveillance, whether it be electronic or other surveillance, so the Congress could be assured that what we are trying to do is in the best interest of the United States.

We are distressed, you know, I am distressed, my colleagues are distressed. I think the individuals in the Federal Bureau of Investigation are distressed, that so often what we think is necessary, and what we feel conscience-bound to do is being misunderstood. We are distressed by abuse by people who are not a part of the intelligence community because of the damage they do to what we consider to be absolutely necessary and an indispensable function of the executive branch.

Mr. KASTENMEIER. Do you concede, Mr. Petersen, that there is abuse by the Federal Government in connection with this?

Mr. PETERSEN. I think—well, I have to concede that there has been at least one abuse, one abusive action. But, I think your statement is too general. Frankly, I am impressed by the lack of abuse in the areas so far as I can see. I do not mean to say, Mr. Chairman, that you and I might share the same judgments, you know, on particular instances. There are instances where Mr. Maroney and I disagree or the Attorney General and I disagree. And ultimately he has made the decision. But, they are not irrational disagreements. They are not circumstances which are so marked that either one of us could say that the other is categorically wrong or being abusive of authority or irresponsible. I do not see that sort of thing.

Mr. KASTENMEIER. Without cataloging them, we are all aware that there have been in the past 2 or 3 years a number of cases of electronic surveillance made public by one means or another, which appear to be abuses to many people.

Mr. PETERSEN. Well, you know——

Mr. KASTENMEIER. I do not want to make it any more specific than that. I do not want to go down the litany of cases, but that is one of the reasons I think both the Senate and the House are presently involved in this inquiry.

Mr. PETERSEN. You see I am not sure whether they are, indeed, abusive. For example, one of the bills here suggested a certain category of persons, justices, judges, Members of Congress, somebody else ought to be excluded. I do not agree with that. You know, I think you are no better or no worse than the rest of us. I think today's paper classifies and illustrates better still the problem. You know, Willy Brandt's chief aide turns out to be a spy. I mean those things do happen. We ought not to exclude categories, newsmen or what have you. Indeed, in the temper of the times, if I were a Russian agent the first thing I would do would be to get myself a newspaperman's job because I can tell you it is much more difficult for us either under an internal security approach or a pure criminal approach to investigate a newspaperman. I think it is wholly unwarranted. It is more difficult for us to investigate a Congressman. It is difficult to conduct an investigation with political connotations, you know. To the extent that you proceed cautiously you may be criticized as I was in connection with the *Watergate* case.

Mr. KASTENMEIER. I might say, Mr. Petersen, that it is difficult for our parent committee to conduct an investigation with political implications.

Mr. PETERSEN. Maybe that is a great safeguard for both of us, is it not?

Mr. DRINAN. Mr. Chairman, may I ask a question?

Mr. KASTENMEIER. Yes. I yield to the gentleman from Massachusetts.

Mr. DRINAN. I appreciate your concern and the concern of your colleagues with this. But, I wonder if you can enable us to make some evaluation on the basis of information other your own statement, by giving to us the evidence that the chairman has requested. I am particularly interested in the number of warrantless wiretaps. I have the previously released statements of Senator Scott and Gerald Ford on the number of warrantless wiretaps prior to 1973; but, I wonder if you could give us now, or hereafter, the number of warrantless wiretaps that have been authorized?

Mr. PETERSEN. Mr. Drinan, I am not prepared to do so.

Mr. DRINAN. We asked for this information in a letter, dated April 11, and we asked for compliance by April 18, and we agreed to a deferrence of that. But, it seems to me that if you are not prepared, then you ought to give us a date when you are prepared.

Mr. PETERSEN. Well, I would like to be able to do it, but I cannot. That is going to have to come from the Attorney General of the United States.

Mr. DRINAN. We wrote to the Attorney General of the United States on April 11, and I have here hearings of the Senate, held 2 years ago, on warrantless wiretaps.

Mr. PETERSEN. Well, you know, all I can say, Mr. Drinan, is I can misconstrue him at times, but I cannot overrule him.

Mr. DRINAN. Are you telling us that Mr. Saxbe has denied our request?

Mr. PETERSEN. I am telling you that at least as of this morning he still has it under consideration, and I have no satisfactory answer for you or myself.

Mr. DRINAN. How do you expect us to say then you feel there has been some abuse, but no grave abuse, when we do not even know the number of warrantless taps?

Mr. PETERSEN. Well, I do not know that I can do other than ask you to accept my representations. I can tell you that and if you want to swear me, I will still say it. But, other than that, I just offer my testimony as a public official.

Mr. KASTENMEIER. If the gentleman from Masachusetts will yield, I think it appropriate that this subject should be pursued. For the record, the letter that was sent to the Attorney General on April 11 contained four questions, and none of those questions have been answered in the testimony this morning. Is that correct, Mr. Petersen?

Mr. PETERSEN. We discussed the procedures.

Mr. KASTENMEIER. You discussed the procedures?

Mr. PETERSEN. Yes.

Mr. KASTENMEIER. The reason I have asked this is so that we can delineate which of the questions are answered in your testimony and which are not. The questions which are not, as you correctly point out, we will have to take up with the Attorney General. Possibly we can resolve this at some future time, but not this morning. Therefore, I think for the record that the Chair will pose each question asked in the April 11 letter and you will indicate whether or not it is still under consideration by the Attorney General, or whether or not your testimony considers it, and if it does, what answer your testimony gives.

Mr. PETERSEN. Okay.

Mr. KASTENMEIER. We asked the Attorney General of the United States, by letter of April 11, for each calendar year from 1969 through 1973, how many requests for permission to conduct warrantless wiretaps or electronic surveillance were granted by the Attorney General. That is the first question.

Mr. PETERSEN. That has not been answered, Mr. Chairman.

Mr. KASTENMEIER. The second question is for each of these years, how many approved requests for permission to conduct warrantless wiretapping or electronic surveillance involved a United States citizen as the chief subject of the surveillance?

Mr. PETERSEN. That has not been answered.

Mr. KASTENMEIER. That third question is: Is a standard procedure used for processing requests for warrantless wiretapping or electronic surveillance, and, if so, what is the procedure?

Mr. PETERSEN. I have just described that procedure orally, so I think that the record will reflect that that is answered and that that is the procedure. I might amplify that a bit. It has varied under attorneys general. Under Attorney General Mitchell, the requests were brought to him and signed by him. Under Attorney General Kleindienst, they were brought to him and he solicited then the recommendation of the Assistant Attorney General of the Internal Security Division or myself at a later date and, under Attorney General Richardson, he handled the matters wholly in his own office. And under Attorney General Saxbe, they followed the procedure I previously described.

Mr. KASTENMEIER. Do other agencies, if so, which other agencies, make such requests for approval by the Attorney General for warrantless wiretapping?

Mr. PETERSEN. As a matter of procedure, any agency which is conducting an internal security investigation, in the broadest sense of the term, and desires information which can only be obtained by a type of electronic surveillance, is required to process that request through the Federal Bureau of Investigation and the Federal Bureau of Investigation will conduct that.

Now, we do not get into activities, foreign activities of other intelligence agencies which take place on foreign soil.

Mr. KASTENMEIER. Is it your answer, then, on the latter point, that all warrantless interceptions that take place within the United States, under the authority of the United States, are processed through the Attorney General, and through the FBI.

Mr. PETERSEN. It is my answer that they are supposed to be and all those that are legitimately done are.

Mr. KASTENMEIER. Whether these are, let us say, within the Defense Department, within the National Security Agency, the Central Intelligence Agency, or whatever agency, and are within the confines of the United States?

Mr. PETERSEN. If the Central Intelligence Agency wanted to cover x in the United States, they would be required to go through the FBI and have the FBI do that in which case it would be authorized by the Attorney General.

Mr. DRINAN. May I intervene?

Was the tap of Dr. Morton Halperin authorized by the Attorney General?

Mr. PETERSEN. Yes, it was.

Mr. DRINAN. You mentioned that there were some abuses. Do you think that that was an abuse?

Mr. PETERSEN. I do not know, Mr. Drinan. My perception is not, but on the other hand, I have to say that has been subjected to rather extensive investigation by the Special Prosecutor, and I have not seen all of the investigative reports. The conclusions reported to me are that while one may differ with the wisdom of the procedure involved, that it was not an abuse, that there was a security problem of considerable dimension. And so, I would have to conclude on the basis of what I know that it was not an abuse.

Now, that brings us to another question: That is. the degree of abuse, or the question of abuse, seems to take on a different meaning depending on who is covered or who is surveilled. For example, let

us assume for the moment that I work for Senator x, and I am a foreign intelligence agent, and the Bureau gets wind of that and they use electronic surveillance to develop precisely what I am doing.

Mr. KASTENMEIER. That is not a very common case that you have just given.

Mr. PETERSEN. No, it is not. But, you see, it is not an uncommon possibility. If you recall——

Mr. KASTENMEIER. Have you had such a case?

Mr. PETERSEN. Senator Muskie had a problem, did he not, in connection with just this very thing, because one of those people who was being surveilled happened to work for him. But, as I told him if I were an agent and I worked for him, the Bureau certainly would not stop surveilling me. So, the nature of the problem is not changed by the fact that I go to work for the New York Times, or I go to work for Congressman Kastenmeier, or I go to work for Senator x. But, the perceptions of that problem are changed, and the need for precision and care and prudence, you know, even for perhaps some disclosures in the legislative branch at an earlier date than possibly might be warranted in order to ensure that what the Executive is doing is not misconstrued.

For example, when we had an investigation of a Supreme Court Justice, we went to the Chief Justice, not because we had to, not because it was not in our power to do it, but because we wanted him to understand, and so that our motives would not be misconstrued. Prudence, yes. Is it mandated? No. Now, if you asked me whether all of these things have been handled prudently, I would say absolutely not.

Mr. DRINAN. Would you give us an example of an abuse? If the tap on Dr. Morton Halperin is not an abuse, then what would be an abuse?

Mr. PETERSEN. Well, I suppose that you would call an abuse, Mr. Drinan, any mistake of judgment. I think that is too stern a test. I am hard pressed to think of any official action where the action was taken purely in an abusive sense, without any regard to governmental responsibility.

Mr. DRINAN. Mr. Petersen, we are hard pressed because this is the only oversight committee in the entire House of Representatives. We have been treated very shabbily by the Attorney General. He has refused to give us the precise basis on which we may evaluate the use of wiretapping, namely, the number of warrantless taps. Would you suggest that the only way that we can get the figures is to subpoena them? I will move that we subpoena them.

Mr. PETERSEN. I do not think, if you will excuse me, that that makes a lot of sense.

Mr. KASTENMEIER. If the gentleman from Massachusetts will yield back, we have been diverted from our original line of questioning to the question of abuse. We can return to the question of abuse later if we like.

Mr. PETERSEN. I did not want to leave that, if you will excuse me, Mr. Kastenmeier. It did not make a lot of sense, period, a lot of sense in the sense that it never seems wise to me to force that kind of a confrontation under the separation of powers doctrine.

Mr. DRINAN. Except we will never get the documents. We will never get the facts.

Mr. PETERSEN. I do not think that is true.

Mr. DRINAN. We have been waiting 2 years, sir; we still just do not have the basic facts of the warrantless taps, which is the essence of all of this.

I yield back to the chairman.

Mr. KASTENMEIER. I was merely stating that we were considering the question in the letter relating to the relationship between surveillance by other agencies and the Department of Justice. The question of abuse is another question. We will return now to the point where I was asking whether all of the agencies of the Federal Government operating within the United States cleared their requests for warrantless taps or surveillances through the Attorney General or through the Federal Bureau of Investigation. You indicated that was the case.

I asked this for informational purposes only. I take it that overseas, whether or not the subjects are American citizens, agencies of the United States might not necessarily clear, electronic surveillance plans through the Department of Justice. Is that correct?

Mr. PETERSEN. Overseas?

Mr. KASTENMEIER. Overseas.

Mr. PETERSEN. I do not perceive that the Attorney General's responsibility is that encompassing. I have to say that that is an individual opinion. I have not discussed it with him and he may have another opnion. But I do not perceive that they are that encompassing, and it does not occur to me that he has, if you will, oversight responsibility with the National Security Agency or the Central Intelligence Agency. I just do not understand that to be the case.

Mr. KASTENMEIER. Yes. The purpose of the question is to try to delineate which procedures we are talking about or which warrantless procedures are not really covered.

Mr. PETERSEN. To the extent that we are talking about citizens overseas, and that is the only instance where I perceive there is a legal question, that legal question is far from clear, whether or not the constitutional guarantees are applicable to a citizen in a foreign country, who may be involved in any suspected activity. That is an answer on which you, or a question on which you may get different answers.

Mr. KASTENMEIER. Under present practice, if an agency did not, in fact, clear its warrantless surveillance through the Department of Justice, is there any penalty for such agency or a person in such agency conducting the surveillance?

Mr. PETERSEN. I would consider that except for those surveillances which followed the mandated government procedures; that is, through the Attorney General, that they would be subject to the penalties of the civil provisions of title III of the Omnibus Crime Act.

Mr. KASTENMEIER. These have been questions which I have added as an extension of question No. 3 in my letter.

The fourth question in the letter is, are there any written directives, memoranda, regulations, or manuals, which set forth proce-

dures or guidelines to be used by investigative agencies in applying for permssion to conduct either warrantless or a court-approved wiretapping or electronic surveillance?

Mr. PETERSEN. So far as title III is concerned, an application for court-authorized electronic surveillance, the procedure, that business about the manual is covered in my statement. We do have a very extensive manual and it is distributed to the appropriate investigative agencies and lawyers concerned with the application. It is for administrative use only. It is obviously not a rule of law. It is what we regard as proper administrative practice in connection with it, and it is very detailed. With respect to national security standards I honestly do not know what internal instructions the Bureau has for its agents. We do have the overall instructions from President Johnson, which continue in effect that all of these things are to be cleared through the Attorney General. Now, obviously, that is a general instruction and does not fall in a manual category.

Internally, after referral, I have described the procedure which takes place in the Attorney General's Office or in the Office of the Assistant Attorney General concerning those matters. I have to say that implementation of this internal security program, and perhaps as a result of current events, certainly the interest of the Congress, Mr. Maroney and I, or excuse me, I did not introduce him before, but I have here Mr. Philip White who is a staff assistant in the Criminal Division, embarked upon a program to try and articulate, if you will, standards, formalized standards, and guidance for those who are concerned with internal security electronic surveillances.

Now, I mention that with some trepidation, you know, because I do not want to disclose it to Congress if we get it, if you will excuse that. I certainly do not want to disclose it to the public at large. I do not want it to be disclosed. I do not want to create a situation where the first thing that a foreign intelligence agent does is look at the standards and see how he can adopt a cover that will take him without those standards. But, there again, it is an attempt to develop some degree of uniformity in the practice.

Now, once again, I go back to the business of oversight. When I say I do not want to disclose to the Congress, I mean I do not want to put it in the Congressional Record and have it promulgated. But, certainly I want to get this across, that we have no objection when we develop these standards and articulate them, to bring them up and show them to a specified group of a select committee to insure, or to persuade them, that what we are doing is in the interest of the United States.

Mr. KASTENMEIER. I can appreciate that there are many things you might want to present to the Congress in say a confidential or executive session, but I think it is somewhat presumptuous, Mr. Petersen, for you to say under what circumstances; that is, what the Congress must do to organize itself for you to agree to do business with us. And that is really what you are suggesting.

Mr. PETERSEN. Well, you know, certainly it was presumptuous to say I am doctrinaire about it, and I certainly do not mean to do that.

Mr. KASTENMEIER. In the sense we must have a Joint Committee, and we must do this or that, and then you might be agreeable to do certain things that you would not otherwise be agreeable to doing.

Mr. PETERSEN. I do not want to be misunderstood on that. I offered in the sense of, in the sense of openness, if you will, and in a sense to indicate to you what we are trying to do. But, again, I am wholly opposed to the idea of confrontation, or dictating to you how it should be done. But, we do deal with different functions, we do deal with Executive authority. And, Mr. Congressman, with all deference, yours is not the power to conduct foreign relations, and yours is not the power of the Commander in Chief. And there is a separation of powers principle there. And if the effectuation of any of those mandated, important, critical, necessary duties would be jeopardized by that type of disclosure, it would be a violation of the Constitution to make that disclosure, whether it be to the Congress or to anyone else. That is what I am trying to get across. And so, when I suggest a procedure it is to avoid confrontation and it is to avoid arrogating to ourselves the power that ought to be shared and the exercise of which ought to be viewed with some degree of confidence. Only in that sense, Mr. Chairman.

Mr. KASTENMEIER. I do not want to moralize about the question either, but the Congress does have the constitutional duty to make the laws of this country, and it has the duty to exercise oversight with respect thereto on behalf of the people. And I would suggest only the lesson of the last 2 years to suggest some humility to the executive branch with respect to its unilateral exercise of power in this country.

Mr. DRINAN. Mr. Chairman, may I follow up on that?

Mr. Petersen, we do not have to reach all of those grave questions to have you give the subcommittee what we have asked for. The President of the United States authorized Senator Scott on June 5, 1973, to request the number of warrantless taps over the past several years, and I read them. There are discrepancies between these figures and figures written by Mr. Robert Mardian on March 1, 1971. I will read the latter figures authorized by the President of the United States, and the bottom line is this, that we have asked that you people furnish the number of warrantless taps in 1973. We are not asking to invade the executive branch of the Government. We are asking for the next figure.

In 1969, warrantless taps, 123; 1970 warrantless taps 102; 1971, 101; 1972, 108. We are simply asking that you supply the figures for 1973. Perhaps we will have to go to Senator Scott and ask him to authorize the President to release the 1973 figures. That is the main one that we want. And I do not think that you should lecture us on the authority of the President to conduct national security surveillance. We are simply trying to do our job, and you are preventing us from carrying out our responsibility of oversight.

Mr. PETERSEN. You know, again, I do not want to be presumptuous, and I did not mean to seem to be lecturing you. But, on the other hand, I thought you expected candor and I wanted to express a point of view. That point of view is not wholly novel. I refer you to Dr. Schlesinger's book on the "Imperial President" in which there are some very interesting statements with respect to the right of the President to take action without the consent of Congress. And the only check on that is subsequent ratification and approval, and it is

clear, as Dr. Schlesinger points out, that the Executive proceeds at its peril. It is a very extraordinary responsibility. But, you know, the problem is there. I do not mean to lecture you. I am trying to——

Mr. DRINAN. Would you give us the figure for 1973 by next week, by Tuesday?

Mr. PETERSEN. Mr. Drinan, if I could give them to you, I would hand them to you right now. I told you that there are approximately 100. I am not permitted to go beyond that. Now, do you want me to violate my orders to the Attorney General? I could not do it if I wanted to. I do not have the precise figures. I will take your message back.

Mr. KASTENMEIER. I think the point is clear that that is a matter within the authority of the Attorney General, and I will accept the point of view that we can take that matter up with Mr. Saxbe, rather than with you, Mr. Petersen.

Mr. PETERSEN. I would not mind having the authority to overrule him if you want to give it to me, but I do not have it.

Mr. KASTENMEIER. The manual which you referred to as having been furnished the Federal agencies, I take it this is a confidential manual?

Mr. PETERSEN. Well, we like to think it is. We are litigating under the Freedom of Information Act. I hope we win, quite honestly, for this very specific reason. Manuals, when promulgated to the public at large, or to defense counsel, have the habit of being translated into principles of law and, therefore, what is structure or guidelines or policies or standards, then comes back to haunt you and for that reason we should just like not to make them made public, but for that reason only.

Mr. KASTENMEIER. The reason I have asked is that we have also requested two copies of whatever manuals, guidelines, regulations or directives used in connection with electronic surveillance be supplied. If there is some difficulty with this, we will have to take that matter up with Mr. Saxbe as well. You may continue or if you have finished with your presentation, I will yield.

Mr. PETERSEN. I am at your service. The Department of Justice opposes every one of those bills for the reasons I have just stated.

I do agree to what has come through on some of these answers, that what we are concerned about is the degree of disclosure and I feel certain if total disclosure were made that we would not be very, very far apart to say the least. But, I will be happy to answer any questions that you have.

Mr. KASTENMEIER. You indicated that you found it difficult to comply with title III but you had worked under it, you were able to do it and were willing to do it, and you do not want to see title III changed.

Mr. PETERSEN. When I say difficult, it takes us—for a period of time it was taking us 12 days to process those affidavits and, you know, under legal standards it almost became stale. We have cut that down to about an average of 5 days, and we are reluctant to do more I think, or to make it any less complex because we want to insist upon the degree of supervision that we now have. Difficult only in that sense. It is a very technical statute, it is a very lengthy statute

and one of my friends from the defense said: "Henry, we are going to litigate you to death on that thing." Well, they may well, but by the same token, we find it operationally effective.

Mr. KASTENMEIER. You also indicated that very few of the applications made for warrant interceptions were denied. As a matter of fact, I read you some figures by the Administrative Office of the U.S. Court, indicating that of 2,751 applications, 6 were denied and 1 was withdrawn, presumably at the request of the court. Some would suggest, not as you suggested at the outset, that you were doing a tremendous job of setting forth your applications, but that the judges are not doing much of a job in reviewing these requests. What is your experience with respect to the critical review by the Federal Courts of these applications for surveillance orders?

Mr. PETERSEN. I have asked that question, too, and the response I get back from the lawyers is that the judges do look at them. But to elaborate on the procedure, that application can be stopped any step of the way so that the lawyer in the field turns down more than his superior. And his superior turns down more than I do. But, when we get them, we do not send them up to the Attorney General if we do not like them. They just go back, and they either do them over, or do them better, or do not do them at all. So, I think that is the reason. It is the refinement process, you know. Every one of these lawyers is proud of his professional ability. None of them like to be told that you are a knucklehead or you missed it, or you do not know probable cause or how could you submit something like that. So, it is a matter of pride involved when they submit it, and they like to think that it is good and it is going to be praised not criticized. And I think that is wholly accounted for by the degree and the depth of review.

Mr. KASTENMEIER. I guess a comparison ought to be made to some other class of applications not dealing with electronic surveillance and one would have to ask whether the courts are more selective in approval.

Mr. PETERSEN. Well, I think there are two things: First of all, I think that if we are going to make a comparison, you would have to make the comparison to some other ex parte proceeding, and the application for a search warrant generally.

Secondly, you have got to be mindful that this is subjected to a judicial review at the trial level on motion, in the course of the trial in terms of the admissibility of the evidence, and finally in terms of appellate review. So, you know, judges, as we all know, do not like to be reversed. I think they do look at them carefully.

Mr. KASTENMEIER. Have there been any renewals?

Mr. PETERSEN. On probable cause?

Mr. KASTENMEIER. Yes.

Mr. PETERSEN. I think maybe one, one or two.

Mr. KASTENMEIER. I have just one further question and that has to do with what prosecutions, if any, has the Department of Justice undertaken for violation of title III?

Mr. PETERSEN. Well, I perceive that we are under the same standards as every other citizen of the United States, so that if an agent

violated title III by willy-nilly installing a wiretap, you know, he would be subject to prosecution. On the other hand, we do not perceive that a failure of probable cause, or a mistake subjects personnel in the Department to prosecution, when they have made a good faith attempt under the statute.

Mr. KASTENMEIER. I am making an assumption that there may have been somewhere in the United States some number of instances where wiretapping and electronic eavesdropping was engaged in, possibly by agents of the Government or otherwise, which were illegal under title III and which might have been prosecuted, and I am asking you how many, if any cases, you have prosecuted?

Mr. PETERSEN. I know of two situations only, two that might conceivably be thought by outsiders to fall in that situation. One was the recently concluded hearing in the Wounded Knee case where there was at issue a party line, and the party line had been installed at the request, or reinstalled at the request of the people, the other side that was in the enclave, and there were at least 10 parties to that line. And in the course of installation, another phone was put in and there was an incidental overhearing in connection with that which led to a protracted hearing after, and the court held that the agent listening in on that party line acted illegally. Now, those in the Criminal Division do not agree with that in terms of the definition of title III but, in any event, that is what the court held. I would not consider that to be actionable in a criminal sense.

The other instance of which I can think is the VVAV Case down in Gainesville, Fla., where there were allegations that there may have been Bureau agents that were found in the telephone frame room in the courthouse. There was an extended hearing on that, and the agents were there to check out as periodically they do, the security of the lines.

Mr. KASTENMEIER. Yes. The implication of my question is, has, indeed, the Justice Department been staffed in terms of prosecuting abuses under title III of wiretapping or electronic surveillance?

Mr. PETERSEN. No, I do not think so.

Mr. KASTENMEIER. In which case I was asking for your records in terms of prosecution.

Mr. PETERSEN. We do not have it, and we will be happy to give it to you. I do not have it at my fingertips, Mr. Chairman. But, we think we have a reasonably good record on that. It is much better than it was under 605, probably because the statute is more effective and most of the cases are against private detectives and lawyers, largely in domestic-relations cases and some commercial espionage. So there are some and at least one investigation is being conducted with respect to State law enforcement officers' actions in one of the States. I think our record is reasonably good on that question, and we will make the figures available.

Mr. KASTENMEIER. Thank you. We would like to have the figures available.

[Subsequently, the following information was supplied by the Department of Justice:]

ANALYSIS OF CASES TERMINATED UNDER THE INTERCEPTION OF COMMUNICATIONS STATUTES[1]

Fiscal year	Statute	Cases terminating in conviction		Cases not terminating in conviction			Tota
		Conviction after contested trial	Plea of guilty or nolo contendere	Dismissal by D.J.	Dismissal by court	Aqcuittal	
1969	18 U.S.C. 2511						
	18 U.S.C. 2512		1(1)				1(1)
	47 U.S.C. 605				1(1)		1(1)
	Total		1(1)		1(1)		2(2)
1970	18 U.S.C. 2511		2(2)				2(2)
	18 U.S.C. 2512						
	47 U.S.C. 605	1(1)		1(1)	4(5)		6(7)
	Total	1(1)	2(2)	1(1)	4(5)		8(9)
1971	18 U.S.C. 2511	1(1)	1(1)		1(3)		3(5)
	18 U.S.C. 2512	2(2)	1(1)	1(1)			4(4)
	47 U.S.C. 605				1(2)		1(2)
	Total	3(3)	2(2)	1(1)	2(5)		8(11)
1972	18 U.S.C. 2511	3(5)	5(7)	1(1)	2(6)	3(3)	14(22)
	18 U.S.C. 2512		1(1)		1(1)	1(1)	3(3)
	47 U.S.C. 605	1(1)					1(1)
	Total	4(6)	5(8)	1(1)	3(7)	4(4)	18(26)
1973	18 U.S.C. 2511	4(5)	12(13)	3(3)		3(3)	22(24)
	18 U.S.C. 2512			1(2)	2(2)		3(4)
	47 U.S.C. 605	1(1)					1(1)
	Total	5(6)	12(13)	4(5)	2(2)	3(3)	26(29)
1974[2]	18 U.S.C. 2511	5(7)	2(6)	2(2)		2(2)	11(17)
	18 U.S.C. 2512			1(1)		1(2)	2(3)
	47 U.S.C. 605						
	Total	5(7)	2(6)	3(3)		3(4)	13(20)
Total for all years detailed above		18(23)	25(32)	10(11)	12(20)	10(11)	75(97)
Total cases terminating in conviction		43(55)					
Total cases not terminating in conviction						32(42)	

[1] The statistics maintained by the D. J. Information Systems Section reflect case terminations for many actions which do not, in fact, represent a final termination of the case, eg., dismissals followed by the filing of a superseding information or indictment and rule 20 transfers. Such nonfinal terminations are eliminated from the statistics above.

[2] Statistics for fiscal year 1974 are based on data through the first 6 months of the fiscal year.

DEPARTMENT OF JUSTICE ACTIVITY UNDER THE INTERCEPTION OF COMMUNICATIONS STATUTES

Fiscal year	Complaints received by FBI [1]	Cases filed (indictments & informations) [2]				Cases terminated [3]			
		18 U.S.C. 2511	18 U.S.C. 2512	47 U.S.C. 605	Total	18 U.S.C. 2511	18 U.S.C. 2512	47 U.S.C. 605	Total
1969 [4]	433	[5] 3(3)	1(1)	3(4)	7(8)	----------	1(1)	1(1)	2(2)
1970	541	3(3)	3(4)	3(4)	9(11)	2(2)	----------	6(7)	8(9)
1971	521	8(12)	2(2)	----------	10(14)	3(5)	4(4)	1(2)	8(11)
1972	541	15(21)	6(7)	2(2)	23(30)	14(22)	3(3)	1(1)	18(26)
1973	569	19(33)	3(4)	1(1)	23(38)	22(24)	3(4)	1(1)	26(29)
1974 [6]	407	11(15)	1(2)	2(4)	14(21)	11(17)	2(3)	----------	13(20)
Total	3,012	[7] 59(87)	16(20)	11(15)	86(122)	52(70)	13(15)	10(12)	75(97)
Cases pending as of Jan. 1, 1974	----------	12(16)	5(7)	2(4)	19(27)	----------	----------	----------	----------
Total of cases terminated and cases pending	----------	[7] 64(86)	18(22)	12(16)	94(124)	----------	----------	----------	----------

[1] The statistics set forth in this category are compiled by the FBI and represent what they classify as "cases received for investigation." This term, defined generally, means all complaints which state a prima facie violation of the Federal criminal statute in question. The statistics are compiled for the broad classification of interception of communications violations, which includes 18 U.S.C. 2511 and 2512 and 47 U.S.C. 605. Separate statistics are not maintained for the individual statutes. A case is categorized under the subject matter of the initial complaint. Therefore, if an interception of communications investigation evolves from an investigation begun in another statutory area, that investigation would not be reflected in these statistics.

[2] Except for the figure set forth for fiscal year 74 and for 47 U.S.C. 605, these statistics exclude superseding indictments and informations. Appropriate statistics have not yet been obtained for the excepted categories to permit the elimination of superseding actions.

[3] The statistics maintained by the D.J. Information Systems Section reflect case terminations for many actions which do not, in fact, represent a final termination of the case, e.g., dismissals followed by the filing of a superseding information or indictment and rule 20 transfers. Such nonfinal terminations are eliminated from the statistics in this category.

[4] Title 18, United States Code, sections 2511 and 2512 became law on June 19, 1968, and 47 U.S.C. 605 was amended to its present form on that date. Therefore, the statistics set forth above cover virtually the entire history of the currently existing interception of communications sttheatutes.

[5] The figure in parentheses represents number of defendants involved in the stated cases.

[6] The statistic as to the number of complaints received by the FBI in fiscal year 74 is based on data through the first 7 months of the fiscal year while all other statistics for fiscal year 74 are based on data through the first 6 months of the fiscal year.

[7] As a result of the elimination of superseding indictments and informations and nonfinal terminations from the above statistics, the total of cases terminated plus cases presently pending should equal the total number of indictments and informations filed. However, as is apparent above, these figures—while close—do not exactly equate. This may be explained, in part, by the lag in data being reported from the field, and, to a small extent, by the occasional failure of United States Attorney's offices to comply with the Department reporting requirements.

DISPOSITION OF APPEALS TAKEN UNDER THE INTERCEPTION OF COMMUNICATIONS STATUTES

Fiscal year	Statute	Cases/ defendants	Disposition
1969		None	
1970		None	
1971	18 U.S.C. 2511	1(1)	Dismissed in favor of United States.
	47 U.S.C. 605	1(1)	Decision in favor of United States.
1972	18 U.S.C. 2511	1(2)	Do.
	18 U.S.C. 2512	1(1)	Do.
1973	18 U.S.C. 2511	1(1)	Do.
	18 U.S.C. 2512	1(1)	Dismissed in favor of United States.
1974	47 U.S.C. 605	1(1)	Decision in favor of United States.

Mr. KASTENMEIER. At this point, I would like to yield to the gentleman from New York, Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman.

Mr. Petersen, pursuing the questions of Father Drinan, regarding figures for warrantless wiretaps for the years of 1969 through 1972, which were disclosed, has there been any problem because they were disclosed?

Mr. PETERSEN. Well, the Bureau did not like it. I think Mr. Maroney testified to some of the figures and they said that if they had known that he was going to do that that they would not have given them to him. So, there has been some internal problem, yes, sir.

Mr. SMITH. Other than the fact that they did not like it, has there been any problem because they were disclosed?

Mr. PETERSEN. They take the position whether you agree with it or not, they take the position that since the *Keith* case, where security covers in the United States, at least, in investigating groups or those that are not clearly foreign-controlled to require a warrant, that the number has an intelligence element now, per se. You know, whether you agree with that or not that is their position and that is the basis for their objection to Mr. Maroney furnishing those figures in the past. And they say that that type of information, since we are so selective, you know, in our use of it, that a minimum number could be of intelligence value to those countries who maintain foreign agents here.

Now, you know, part of the difficulty we have, Mr. Smith, is this: We are talking about approximately 100, as I told the chairman earlier. I have said that I cannot prove this, but as contrasted with that, we are talking about 75,000 of these installations in another Western European country. Now, that is a remarkable difference.

Mr. SMITH. Is that what we are talking about?

Mr. PETERSEN. Maybe they are wholly unrestrained. I do not know.

Mr. SMITH. And we are talking about possibly 100?

Mr. KASTENMEIER. And we are talking about possibly 100. Now, maybe they are wholly unrestrained but even if they are 700 percent unrestrained, it is still a remarkable difference.

Mr. SMITH. Because there is thought to be some intelligence concern, is this the reason that the Attorney General has not met our request as set forth in paragraphs 1 and 2 of the letter of April 11?

Mr. PETERSEN. Well, I assume so. I did not want to impute that to the Attorney General categorically without—I was out of town

until late last night, and hence I did not get the opportunity to discuss it with him yesterday, this specific point, and we had proposed to do it today, and again today I did not have the opportunity. But, I had to assume that that is the basis for his position.

Mr. SMITH. I would like to suggest, Mr. Petersen, that when you do discuss it with him that you might perhaps look at the possibility of how these figures might be furnished to us, perhaps in executive session of this committee or something like that?

Mr. PETERSEN. I would be delighted to do that, of you all do not perceive that I am trying to tell you how to run your business, Mr. Smith.

Mr. SMITH. Now, let me get briefly to where Senator Gaylord Nelson had introduced one of the bills that is before this committee would require a court-issued warrant on probable cause in order to authorize an electronic surveillance which is now called warrantless wiretap. And you have stated categorically the Department is opposed to it. Why would you be opposed to it?

Mr. PETERSEN. Well, I am opposed to it for this reason; first of all, I think that the judge lacks the factual background information and expertise in the area that I think is necessary. Secondly——

Mr. SMITH. But at that point is he not only deciding on the probable cause being testified to him by experts?

Mr. PETERSEN. You anticipate me.

Secondly, I do not agree that probable cause is the proper standard. The Supreme Court has suggested in one of its cases that perhaps some lesser standard could be employed. We have had great difficulty in trying to articulate a lesser standard. By the same token, however, the court in the *Ivanov* case clearly indicated that suspicion as opposed to probable cause was a satisfactory criteria. I can tell you my own standards in approving these things, or of not approving them for that matter, is to apply a standard of suspicion and need to the extent that I can ascertain the need, and it is difficult for me, you know, because I am not immersed in intelligence every day. So, I would say that when you couple one detachment of the court with probable cause, while those factors are ordinarily quite efficacious in criminal matters, I think that they would not serve the purpose here.

Now, if we apply standards of suspicion and need, the question then seems to me to be a matter of control. Now, that control I think has to be exercised by those who have a keen appreciation of those factors which constitute suspicion and which constitute a need. And I do not think that you and I are likely to get that degree of expertise in the court. That is the reason that I suggest that if there is going to be any procedure in that fashion that it be in some type of commission which has the responsibility on a day-to-day basis, so that they could develop this degree of insight that is necessary. Now, we have all seen the criticisms that arise from intelligence failures. Whenever there is an upheaval in the Middle East there is at least public criticism, or commentary, perhaps, that well, we knew, or we did not know, and if we did not know why did we not know. And how could the President be expected to take the proper courses of action if the CIA or other intelligence agencies failed in

their responsibility to bring it here, bring you information? So, it does require a great deal of vision to fix foreign policy positions, and it is one of the functions that I am told that the National Security Council and the United States Intelligence Board do have. These factors concern the national interest of the United States and fix the patterns for the direction and the general policy directives of the intelligence agencies involved.

Now, that is too much to try to translate to a judge or to someone who operates on a haphazard basis. And you may well say, on the other hand, it is too terrible a weapon to leave wholly with the investigative agencies subject only to the review of political appointees. Well, perhaps they are reasonable positions. All I am suggesting is that if there are alternatives they have not been cast in terms of probable cause by courts, particularly, when almost every court that has concluded that, that has examined this in its foreign policy and foreign intelligence implications has agreed with the Government—that under the fourth amendment standards a lesser guideline may be employed where foreign intelligence or foreign relations are involved. And the latest impaneled decision by *Ivanov* is clearly supportive.

I took great consolation from reading that opinion because it reinforced me in what we were doing. Undoubtedly, the case will go to the Supreme Court and perhaps we will get a further expression of view on the subject.

Mr. SMITH. Thank you, Mr. Petersen.

Mr. KASTENMEIER. Does the gentleman from Massachusetts have additional questions?

Mr. DRINAN. Thank you, Mr. Chairman.

Mr. Petersen, Elliott Richardson, testifying in the other body on April 3, 1974, indicated that he had directed the Department of the Justice and the FBI to undertake a joint review of the electronic surveillance procedures. And Mr. Richardson said that that review was well underway when he resigned last October. Has the Department of the Justice and the FBI continued that joint review of electronic surveillance procedures and, if not, why?

Mr. PETERSEN. Well, first of all, I do not know how far it was under way——

Mr. DRINAN. Mr. Richardson said it was well under way.

Mr. PETERSEN. Well, you have to ask him what was, whatever was underway. I have not been able to find that, and it has not been made available to me. And I have been saddled with the responsibility of conducting that study and I alluded to it earlier. We are in the course of doing that and we are trying to formulate that standards. But, it is now well underway and it is predicated on suspicion, on need, on the standards enunciated by the Congress in 2511, and we are trying to refine that for the guidance of the Agency and the Attorney General's Office. It has not been completed.

Mr. DRINAN. Mr. Petersen, on a related question, one of the basic reasons why Elliott Richardson was so concerned about this and also the reason why you said that you and your colleagues are deeply concerned, and why the Nation is so concerned, is that around the time of Mr. Elliott Richardson's confirmation, it was revealed that

certain wiretap activities had been conducted at the direct request of the White House, and that those surveillances were handled outside of the normal procedures and channels. Can you guarantee to us now that there are no wiretaps that are handled outside of the normal procedures and channels? I do not know the procedures and channels, and that is why we wanted the number of warrantless taps. We do not know where this record is kept. Senator Scott did not indicate the source from which his statistics were taken, and you will have to give us the evidence that we need in executive session so that his oversight committee of the Congress can be assured and can assure our colleagues around the country that there are no wiretaps being handled outside of the normal procedures and channels.

Mr. PETERSEN. Well, I can assure you that no wiretaps should be. I can never, and under any circumstances and under any set of guidelines, assure you that none will. The technique is too generally known,

Mr. DRINAN. What about right today? Are there any wiretaps asked for by the White House—do not shrug, I want evidence. This is the key question, sir. This is the reason why this Nation is in turmoil over the executive branch of the Government admittedly, openly, having to concede that they had authorized electronic, warrantless taps that have been handled outside of the channels of the Department of Justice.

Mr. PETERSEN. Mr. Drinan, in 1965 on June 30, President Johnson issued an order which is still in effect. It said no Federal personnel is to intercept telephone conversations within the United States by any mechanical or electronic device without the consent of one of the parties involved, except in connection with investigations related to national security and no interception shall be undertaken or continued wihout first obtaining the approval of the Attorney General. That is in force now. I cannot guarantee you that that is not breached. I cannot guarantee you that some Congressman or some Senator or some member of the executive branch, or some investigative agency has not gotten himself one of those little devices and gone out and installed it someplace. That is impossible, and that will be impossible under any set of guidelines.

Mr. DRINAN. That is not my question, sir.

Mr. PETERSEN. Well, but your question is susceptible to that.

Mr. DRINAN. No, my question——

Mr. PETERSEN. Under any set of guidelines that is possible. But, I am telling you that I know of no instance.

But, on the other hand, Mr. Drinan, if somebody is going to do that they are not going to come and tell me, because I am going to say you cannot do it. So, there is no way that I can guarantee you ever that I am going to know when there is abuse. Like you, I find out when there is abuse, when for one reason or another the abusers are ineffective and it becomes known.

Mr. DRINAN. Mr. Petersen, a subsequent question: Mr. Elliott Richardson and many others have said that under the *Keith* decision, they feel that the Government should establish a policy that would

require a warrant for any electronic surveillance on an American citizen. What is your opinion on that?

Mr. PETERSEN. Well, as I did not agree with it when Mr. Richardson said it, I do not agree with it now. I do not think the fact of citizenship ought to be determinative. It seems to me that it is much more rational to talk about a reasonable basis for suspicion and need.

Well, let us take a deep cover agent who comes over and becomes naturalized. Should that be a factor? I do not think so. I do not think it is rational at all. Or, a natural born citizen. I do not see that that is a criteria, a proper criteria to apply.

Mr. DRINAN. Mr. Petersen, title III, as you know, authorizes the use of warrants for such crimes as espionage, sabotage and treason. In order to avoid the deep suspicion throughout the country and in the Congress of the number and extent of warrantless taps, would it be a serious inconvenience for you to take advantage of title III, and secure the warrant for alleged crime of espionage, sabotage and treason, and related crimes? And if it would be a serious inconvenience because you would have to reveal the nature of this tap after it was done, would you think that the Congress could pass a bill tightening up title III, having a separate, lesser, weaker standard for those, even American citizens, who are allegedly involved in certain kinds of espionage?

Mr. PETERSEN. Well, I would suppose that you can.

Mr. DRINAN. Why are you opposed to it if we can?

Mr. PETERSEN. Well, I did not say that. I said that I was opposed——

Mr. DRINAN. You are opposed to every bill that has been proposed.

Mr. PETERSEN. Well, I think that is correct. I tried——

Mr. DRINAN. You are opposed to any change in the law.

Mr. PETERSEN. No, I did not say that.

Mr. DRINAN. Any change that has been proposed.

Mr. PETERSEN. No, I did not say that.

Mr. DRINAN. You are opposed to every bill that is here on my desk.

Mr. PETERSEN. I did not say that. Now, if you want to get to what I did say, I will be happy to do so.

What I did say is that I think it would be ineffective to utilize the probable cause standards and the court standards of title III in connection with investigations which have a foreign policy or a foreign intelligence purpose. Now, espionage is not the be-all and end-all of an intelligence investigation. There are other elements involved. If we were involved in wholly a sabotage caused by a citizen at, we will say, one of the plants of the big three automakers, in all probability we would use the title III procedures. But, we would not want to use title III procedures where the saboteur was an agent of a foreign power. We would not want to make that disclosure. We would want to keep our options open. We would want to have the right to use that for intelligence or not, as we chose. Criminal prosecution then would be the last in a series of priorities. We would like to be able to determine whether or not we could make an exchange for some of the elements of importance to our

foreign power, or perhaps one of our agents who is a citizen. I mean, we would like to have all of those options open.

But, I do not mean to testify or leave you with the impression that I am opposed to change simply in those terms. That is the reason I am suggesting, if you will, that perhaps we can rewrite this in terms of a commission, in terms of individuals who are appointed, one by the Congress, one by the Executive, one from the intelligence community who would sit in judgment on these things on a day-to-day basis, and have the expertise and the background and the time to explore all of these issues.

Mr. DRINAN. Mr. Petersen, would you agree with the *Keith* decision encouraged legislation to tighten up the standards so that at least American citizens would have the right under the fourth amendment to have a warrant issued for any surveillance that may be directed toward them?

Mr. PETERSEN. I certainly agree it made the suggestion, yes.

Mr. DRINAN. And that is what we are trying to do. We are just trying to follow the suggestion.

Mr. PETERSEN. I do not object to what you are trying to do by any means, Mr. Drinan. Indeed, I applaud it. It is terribly important. I said before we do not want to carry this responsibility alone, but we do want to insure that whatever is enacted is not by its nature to defeat the very ends which we are trying to attain.

Mr. DRINAN. But aside from the ambiguous suggestion of some floating commission, you have nothing to suggest to us as to how we can carry out the objectives that you embrace?

Mr. PETERSEN. Well, I think that what—what we are talking about is the interjection of a relatively impartial authority between the manipulators of these devices, if you will, to insure against political abuse or executive abuse, that that commission suggestion does the same thing as a court. You know, you could call them court judges, if you want. There is no magic to the title. We are talking about the function.

Mr. DRINAN. That function is precisely located in the Judiciary Committee of the House of Representatives, which has oversight with respect to the Department of Justice, and that is what we are trying to exercise.

One last question: On page 24, you say H.R. 9949 proposes to limit this constitutional power by excluding burglary or any other illegal act from the scope of measures the President or anyone acting or purporting to act on his behalf is authorized to utilize to protect the national security. You are opposed to that bill. Do you suggest that the President can commit burglary?

Mr. PETERSEN. Well, I think that is rather unfair. You know I am opposed to it.

Mr. DRINAN. Why are you opposed?

Mr. PETERSEN. I did not say that I was in favor of burglary. Burglary, you know, is something very special.

Mr. DRINAN. Why are you opposed to it?

Mr. PETERSEN. For one thing the statute ought to speak about breaking and entering, if that is what you have in mind. We are not in there to steal the personal property of another when we go in

there. If we have to use a break-in entering technique to install an electronic listening device, I think that that probably stands on the same basis as an overhearing on an internal security grounds. I did not say that I was in favor of burglary. I said that I was opposed to the bill because if there is an unauthorized burglary, it is covered by the laws of every State. I mean, the classic example is the Fielding break-in. There is no problem with going after that, either under the civil rights laws or the laws of the State of California. I mean, we are not here to proliferate legislation. We simply do not need it. That is my testimony.

Mr. DRINAN. All right. Thank you very much.

Mr. KASTENMEIER. Mr. Petersen, you have been here a long time.

Mr. PETERSEN. And you wear me out.

Mr. KASTENMEIER. And you have been a good witness, and I think this is a very good introduction to the dialog which I assume will continue between the subcommittee and the Justice Department. We appreciate your testimony.

Mr. PETERSEN. Mr. Chairman, it is a pleasure to see you and to discuss and discourse with all of you gentlemen, and however much we disagree I can tell you that we would like and we feel we need your support.

[The statement of Mr. Petersen follows:]

STATEMENT OF HENRY E. PETERSEN, ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION

Mr. Chairman: My name is Henry E. Petersen, I am the Assistant Attorney General in charge of the Criminal Division of the Department of Justice. I appreciate the opportunity to appear before this Subcommittee on behalf of the Department to present the Department's position on H.R. 1597, H.R. 9698, H.R. 9781, H.R. 9815, H.R. 9949, H.R. 11629, H.R. 11838, and H.R. 13825.

The purpose of these bills is to amend portions of statutes relating to the interceptions of wire and oral communications Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2510–2520, authorizing the use of electronic surveillance, is the object of these proposed bills. These various sections of the Omnibus Crime Control and Safe Streets Act of 1968 differentiate between electronic surveillance in instances unrelated to national security interests, and surveillances involving the national security. The former surveillances, which we commonly designate Title III surveillances, are authorized only for classes of crimes carefully specified in Section 2516 of Title 18, United States Code. These are subject to prior court order and are guided by detailed and particularized procedures necessary to obtain such an order, as well as carefully circumscribed conditions for their use set forth in Section 2518. The latter surveillances pertain to national security matters, both foreign and domestic. These surveillances are mentioned in Section 2511(3). There are, however, no prescribed procedures for national security surveillances in Section 2511(3).

The Omnibus Crime Control and Safe Streets Act represents a comprehensive attempt by Congress to promote more effective crime control while protecting the privacy of individual thought and expression. Its enactment reflects congressional recognition of the need for surveillance in combatting various types of crimes, and organized crime in particular. We maintain that electronic surveillance techniques are, to date, the most effective method to bring criminal sanctions against organized criminals, and are indispensable in developing witnesses with corroborating testimony, and generally in providing a useful tool in the evidence-gathering process. The Department's most notable success with the use of electronic surveillances has been against organized crime controlled gambling enterprises. However, surveillances have also proved extremely useful in detecting and arresting violators of the other crimes

listed in Section 2516 of Title 18. Our successes require us to recommend that Title III remain unchanged.

The proponents of these proposed bills appear to believe that electronic surveillances, under the Title III guidelines, violate fundamental constitutional rights by infringing upon personal security. However, much of Title III was drafted to meet the constitutional requirements for electronic surveillances set out in *Katz* v. *United States*, 389 U.S. 347 (1967), and *Berger* v. *New York*, 388 P.S. 41 (1967). The *Katz* decision looks to the Fourth Amendment in inquiring into the "reasonableness" of the search and seizure. The *Berger* opinion sets out the framework within which electronic surveillance may constitutionally be used. The decision of which is paramount, justice of privacy, is not an easy one and can only be balanced by consideration of the needs and conditions which exist at any given moment. The Supreme Court has set out a structural framework to balance privacy and justice, and Title III was enacted within this framework. We believe that Title III is a workable solution arrived at to balance justice and privacy.

Before discussing the Department's position on the proposed amendments, I would first like to review for you the administrative techniques and procedures presently in effect within the Department designed to comply strictly with the electronic surveillance statutes and to centralize control over the surveillance procedures. These procedures and techniques are as follows:

Approval of the Attorney General or a specially designed Assistant Attorney General;

A written sworn application containing a complete statement of facts establishing probable cause relied on by the applicant to justify his belief that an order should be issued;

Findings of probable cause by the issuing judge before entering an order;

A statement in the order of the period of time during which the interception is authorized, which must be no longer than is necessary to achieve the objective of the authorization, and in no event more than thirty days;

A finding by the issuing judge that normal investigative procedures have been tried and failed, or reasonably appear unlikely to succeed if tried;

The recording on tape or other comparable device of all interceptions in such a way as to protect the recording from editing or alteration;

The filing of an inventory of persons named in the order within ninety days after termination of the period of an order;

The filing by the Attorney General in January of each year with the Administrative Office of the United States Courts of a detailed report regarding each application for an order during the preceding calendar year.

In order to insure strict compliance with these and other provisions of the statute. we have established a number of administrative procedures to achieve centralized control over the initiation of interception procedures. Briefly, these procedures are as follows:

Requests for authorization for an interception order must be made in writing to the Attorney General from the highest ranking officer of the investigative agency having jurisdiction over the offense involved;

All requests are initially reviewed in the field by attorneys of the Department of Justice, usually Strike Force attorney of the Organized Crime and Racketeering Section of the Criminal Division, or by a United States Attorney or an Assistant United States Attorney, who assist the investigative agencies in the preparation of the affidavit and prepare the proposed application and court order;

All requests are next submitted to the Organized Crime and Racketeering Section or the Narcotic and Dangerous Drug Section of the Criminal Division where there has been established a special unit of attorneys whose primary function is to review the entire matter for both form and substance, with particular emphasis on assuring strict adherence to the required statutory standards;

When approved by this unit, requests are next submitted for review to either the Chief or Deputy Chief of the Organized Crime and Racketeering Section or the Narcotic and Dangerous Drug Section. If approved here, requests are next submitted for review and approved by the Assistant Attorney General, Criminal Division, and finally to the Attorney General. When so approved by the Attorney General, a letter is prepared authorizing the attor-

ney named in the request for authorization to apply to the court for an interception order.

In addition, we have published and distributed to all Divisions of the Department of Justice, to all United States Attorneys, and to all appropriate investigative agencies a "Manual for Conduct of Electronic Surveillance" which sets forth in detail the procedures that must be followed with regard to every interception pursuant to court order, no matter in which agency of the Government or Division of the Department of Justice it originates. The procedures set forth in the Manual cover every phase of the interception process—from authorization by the Department of Justice through the securing of an interception order and the conduct of the interception itself to use of the information obtained.

As you can see, these procedures are well-structured to accomplish a thorough examination of the necessity to intercept wire and oral communications. Once the need for interception is established, then and only then will the Attorney General or a designated Assistant Attorney General authorize an application for the interception to be presented to the court. In this way, it is impossible for frivolous and unrestrained applications to intercept communications to proceed for court approval.

To assist the Subcommittee, I would like to present the Department's views by first giving a brief synopsis of a bill, and second, by stating the position of the Department in respect to that bill.

H.R. 1597 proposes to amend Section 2511 of Title 18 by requiring ". . . the written authorization of the President specifically authorizing the particular interception or disclosure," when ". . . a judge or justice of the United States or a Senator or Member of Congress is a party. . . ." Section 2511 presently prohibits the interception and disclosure of wire or oral communications unless compliance is made with the electronic surveillance statutes. Strict adherence to these statutes prevents unscrupulous and indiscriminate invasions of privacy.

I assume that this bill is not attempting to substitute a written Presidential authorization in lieu of a Judicial authorization for a wiretap order, but is intended to supplement those procedures in Sections 2516(1) and 2518(1), described above. H.R. 1597 appears to suggest that these existing controls no longer insure sufficient protection of the privacies of specially categorized persons, that is, a United States judge of justice or a Senator or Member of Congress. We disagree.

There is no reasonable basis for distinguishing these persons from United States citizens in general. The unauthorized infringement upon constitutional freedoms must always be prohibited, whether the freedoms involved are those of the persons specially enumerated or anyone else's. Title III has met this challenge by (1) instituting a carefully circumscribed procedure antecedent to the intrusion, (2) implementing the exclusionary rule, (3) making unauthorized surveillance a serious crime, and (4) providing a civil action in 18 U.S.C. 2520 to sufficiently compensate for any unconstitutional intrusion by means of electronic surveillance.

This bill would create preferential treatment for a select few and would expand existing controls which already conform with Fourth Amendment standards. The impartiality of a neutral Judge provides the ultimate examination of the probable cause necessary to prevent unreasonable searches and seizures. This is the case whether the request for wire or oral interception is last examined by the Attorney General or the President.

For these reasons, the Department of Justice recommends against enactment of H.R. 1597.

H.R. 9667 and H.R. 9698 will be considered together. They both propose amendments to Sections 2511(2)(c) and (d) requiring the consent of all parties whose communications are intercepted. Sections 2511(2)(c) and (d) of Title 18, United States Code, now provide that it is not unlawful to intercept wire and oral communications "where such person is a party to the communications or where *one* of the parties to the communications has given prior consent to such interception." (emphasis supplied). These bills desire to alter these clauses to make the consent of parties a necessary prerequisite to interception under these subdivisions of Section 2511(2).

The proposed modifications, in essence, provide that the consensual monitoring of wire and oral requirements of a third party intercepted unless the consensual monitoring was conducted with prior notice to all parties to the conversation. This would negate any efforts to obtain evidence by investigative procedures that have consistently been approved by the Supreme Court.

Court decisions have for some time distinguished between electronic surveillance of conversations without the consent of any of the parties, which requires a court order and a showing of probable cause, and the monitoring of conversations with the consent of one but not all of the parties. *United States* v. *White*, 401 U.S. 745 (1971); *Lopez* v. *United States*, 373 U.S. 427 (1963); *Rathburn* v. *United States*, 355 U.S. 107 (1957); *On Lee* v. *United States*, 334, U.S. 747 (1952). The primary difference between nonconsensual electronic surveillance and consensual monitoring is that in the latter, one participant in the conversation may be collaborating with the Government and may relate to the Government the substance of the conversation. The monitoring serves to provide instantaneous communications and to assure effective corroboration. No information is acquired which would not have been obtained without the accompanying monitor; this method is simply faster and more probative. As the Supreme Court said in *United States* v. *White*, 401 U.S. 745 (1971), we should not:

"* * * be too ready to erect constitutional barriers to relevant and probative evidence which is also accurate and reliable. An electronic recording will many times produce a more reliable rendition of what a defendant has said than will the unaided memory of a police agent * * *. Considerations like these obviously do not favor the defendant, but we are not prepared to hold that a defendant who has no constitutional right to exclude the informer's unaided testimony nevertheless has a Fourth Amendment privilege against a more accurate version of the events in question. 401 U.S. at 753."

The most reliable and probative evidence is always preferred in the law. Science through electronic surveillance techniques can promote the acquisition of such evidence without subjection to the vagaries and frailities of human nature. Where informants, whose credibility may be suspect, are used, where victims of crime are engaged in key conversations with the perpetrators themselves, or where the investigators as such are individually involved and their credibility will be significant factor in the subsequent trial, recorded and monitored conversations are of the utmost importance. Recorded conversations produce the precise character of the spoken words with the inflections, emphasis ,and other aspects of oral speech.

For these reasons, we strongly oppose both H.R. 9667 and H.R. 9698. We further recommend following the American Bar Association's adoption of 18 U.S.C. 2511(a)(c) and (d) as their Minimum Standard of Criminal Justice relating to consensual overhearing and recording. See American Bar Association Standards for Criminal Justice, *Electronic Surveillance*, Standard 4.1, and Commentary, pages 12–13 (1971).

H.R. 9781 also proposes to amend Section 2511, and in addition, Sections 2512, 2516, 2517, 2518, 2519, and 2520 of Title 18, United States Code. This bill suggests that the current procedural safeguards designed to prevent the abuse and misuse of interceptions of wire and oral communications are inadequate and tempt Government officials to further partisan political goals by means of wire and oral electronic surveillance. Further, H.R. 9781 declares that electronic surveillances have been employed too extensively, thereby spawning the undermining of personal security and the violation of the constitutional rights to free speech, press, and association, the rights to due process and equal protection, and the right to privacy.

To correct these alleged infringements, H.R. 9781 proposes, first to amend Section 2511(1) to prohibit *all* interceptions and disclosures of wire and oral communications. Further, a new subdivision (e) to Section 2511(1) is suggested which would prohibit the willful interception or recording of wire or oral communications without the consent of all parties to the conversations.

Second, the bill seeks to strike out Sections 2511(2)(a)(ii), (b), (c), and (d). This would prohibit any disclosure or technical assistance by an employee of a communication common carrier, whose employment may require an incidental wire interception, to a person lawfully authorized to intercept

such. It would also make unlawful the interception of wire or oral communications, the disclosure, or use of such interceptions, by the Federal Communications Commission in the normal course of its responsibilities. Consistent with the proposed addition of Section 2511(1)(e), the elimination of Section 2511(2)(c) and (d) would make unlawful the interception of wire and oral communications where one party to the conversation consents to such monitoring.

Third, H.R. 9781 proposes to strike out Section 2511(3). This seeks to curtail the constitutional power of the President to obtain the intelligence information he deems necessary to protect the security of the United States by the interception of wire and oral communications.

The fourth proposed amendment included in H.R. 9781 would prohibit all manufacture, distribution, possession, and advertisement of wire and oral communication interception devices by amending Section 2512(1). It would also strike out the provisions in Section 2512(2), thereby making it unlawful for a communications common carrier or an employee, a person under contract with such carrier, or an employee of or person under contract with a Governmental body to transport through interstate or foreign commerce any electronic, mechanical or other device primarily useful in the surreptitious of wire or oral communications.

H.R. 9781, lastly, proposes to amend the interception statutes by striking out Sections 2516, 2517, 2518, 2519, 2510(9). These proposals prohibit the authorization and disclosure for interception of wire and oral communications, and eliminate the need for a procedure for the interception and reports concerning the intercepted communications.

As you can see, the ultimate effect of H.R. 9781 is to literally destroy the Government's authority to apply for wire and oral interceptions. The first proposed amendment to the bill recommends that all interceptions and disclosures be prohibited unless the consent of all parties to the conversation is obtained. We object to the passage of this proposal for the same reasons we objected to H.R. 9667 and H.R. 9698. Furthermore, the absolute prohibition on non-consensual interceptions and disclosures undermines the purposes for which the electronic surveillance statutes were enacted. The statements made before this Subcommittee, both now and in the past, have amply demonstrated the need for interceptions of wire and oral communications, and the results obtained from the use of these interceptions.

The second proposal in H.R. 9781 involves forbidding employees of communication common carriers or of the Federal Communications Commission to provide assistance for an interception, to intercept, or to disclose or use the interception. We also object to the passage of this proposal. As our position strongly favors the perpetuation of the electronic surveillance statutes in their present form, any attempt to frustrate the effective execution of these statutes must be strongly opposed by us.

I would like to defer discussion of the third proposal in H.R. 9781 to later discussions of H.R. 9949 and H.R. 13825, all involving national security.

H.R. 9781 also suggested a fourth proposal to proscribe the manufacture, distribution, possession and advertisement of wire and oral interception devices, as well as the interstate or foreign transportation of such devices. Obviously this proposal would prevent any interception of wire and oral communications. As previously stated, we cannot adhere to a policy that would undercut an effective source of crime detection. We, therefore, object to this amendment also.

The last amendment proposed in H.R. 9781, recommends that Sections 2516, 2517, 2518, 2519, and 2510(a) be struck from Title 18. As these Sections set out the procedures for the authorization, the interception, disclosure and use of intercepted communications, and for the reports concerning intercepted communications, their elimination would seriously hamper criminal investigative techniques. By striking these Sections from the electronic surveillance statutes, the Government's authority to seek court approval for wire and oral inerceptions is revoked.

For the above-stated reasons, the Department objects to the passage of H.R. 9781, and to any of the proposed portions of H.R. 9781.

H.R. 9815 and H.R. 11629 will be examined together as they are substantially identical bills proposing a "Freedom from Surveillance Act of 1973."

These bills would prohibit the use of the Armed Forces or any state militia to investigate or maintain surveillance of civilians, except where the use of the Armed Forces is employed to carry out certain specific responsibilities. The surveillance to be curtailed includes monitoring by wiretapping, electronic eavesdropping, overt and covert infiltration, and civilian informants. To accomplish this purpose, these bills seek to add a new section to Title 18, United States Code. They would also amend Title 28, United States Code, by authorizing civil actions for damage and injunctive relief, and by permitting class actions to be initiated to enjoin such surveillance. The bills would also affect the Posse Comitatus Act, 18 U.S.C. 1385, by expanding its scope to include the Coast Guard.

We would point out that this proposed amendment of Title 18, United States Code, is inconsistent with Public Law 90-331, authorizing the use of the Armed Forces to conduct surveillance monitoring when the Armed Forces assist the Secret Service in protecting the President, Vice-President, and foreign visitors.

The Department of Justice believes that the criminal penalties provided in Section 2 of these bills are overly broad. Furthermore, we oppose Section 3 of these bills which authorizes civil actions for damage and injunctive relief. Civil damages are authorized in Section 2520 of Title 18, whenever communications are intercepted, disclosed, or used in violation of this chapter. The addition of the proposed civil remedies in Title 28 would necessarily be superfluous and could be used for harassment to test the authorization of an exception to the surveillance prohibition, thereby increasing the already burdensome load of civil litigation.

We do object to the inclusion of the Coast Guard in the Armed Forces, and urge that the Coast Guard be excluded from the Posse Comitatus Act. Section 5 of these bills, is, therefore, objectionable to the Department as it would prevent the Coast Guard from pursuing its traditional law enforcement duties. See 14 U.S.C. 89.

These reasons force the Department of Justice to oppose the enactment of H.R. 9815 and H.R. 11629.

H.R. 11838 proposes to amend Section 2516(1) and (2) of Title 18, United States Code, to assure that all authorized interceptions of wire and oral communications receive prior court approval. This language of the bill restricts itself to amending Sections 2516(1) and (2). It does not refer to Section 2518(7) of Title 18, United States Code, which provides:

Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—

(a) an emergency situation exists with respect to conspiratorial activities threatening the national security interest or to conspiratorial activities characteristic of organized crime that requires a wire or oral communication to be intercepted before an order authorizing such interception can with due diligence be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception, may intercept such wire or oral communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire or oral communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

H.R. 11838 appears to be directed at the elimination of this emergency provision, but does not accomplish this stated purpose.

We believe that, although the Department has never used this emergency provision, it should be retained without limitation or change. The provision permits investigation to proceed when an emergency situation exists, follow-

ing up this investigation within forty-eight hours with an application to the court to approve such interception. A court order is required as a condition precedent to the use of any intercepted evidence, thereby a sufficient safeguard to potential abuse.

This bill does not, therefore, accomplish its stated purpose. The Department of Justice does, however, object to any limitation on the emergency authorization in Section 2518(7), and objects to the use of H.R. 11838 to attempt to limit this Section of Title 18.

The last two bills pending before this Subcommittee are H.R. 9949 and H.R. 13825, both concerning the authorization of intercepted communications in national security cases. Previously, I deferred discussion of H.R. 9781, Section 2(5), until these two bills were presented, as it, too, deals with national security interceptions.

Each of these proposed amendments would substantially change the language, intent, and effect of Section 2511(3) of Title 18, United States Code, the present recognition of national security authority for interception of wire and oral communications. Section 2511(3) provides that the constitutional power of the President shall not be limited or restricted whenever he deems it necessary affirmatively to act to protect the national security of the United States. Such affirmative measures by the President may include the authorization of wire and oral interceptions, without prior or subsequent court approval.

H.R. 9781, Section 2(5), seeks to wholly abrogate the President's constitutional power by striking out Section 2511(3). H.R. 9949 proposes to limit this constitutional power by excluding burglary or any other illegal act from the scope of measures the President, or anyone acting or purporting to act on his behalf (is authorized to utilize to protect the national security. H.R. 13825 seeks to amend Section 2511(3) by curtailing the constitutional power of the President to act in the name of national security only against foreign agents and powers pursuant to the proposed Section 2518A. The contents, or evidence derived therefrom, of interceptions under Section 2511(3) would not be admissible in evidence nor be otherwise disclosed in any trial, hearing, or other proceeding in Federal or state court, with the exception of admissibility in civil proceedings against foreign agents. Further, H.R. 13825 proposes to delete subsection (a) of Section 2516 of Title 18, United States Code, renumber the remaining subsections, and add a new Section 2516 following Section 2516 concerning the authorization for interceptions in national security cases. Another recommended amendment of this bill would add a new Section 2518A immediately following Section 2518, involving the procedure for interception in national security cases.

H.R. 9949 provides that no Congressional enactment shall be deemed to authorize the President, or anyone acting or purporting to act on his behalf, to engage in burglary or any other illegal act. The Department objects to the enactment of this bill as it would be needless.

It seems fairly obvious, I believe, that the Department opposes the passage of H.R. 9781, Section 2(5), which seeks to destroy the President's constitutional authority to intercept certain communications in the interest of national security. Any limitation of the Presiden's constitutional power to protect the United States against foreign instigated subversion must be objected to. We believe that the deletion of Section 2511(3), although it certainly would not detract from the President's constitutional powers, should be prevented in order to be compatible with constitutional and case law standards balancing the First and Fourth Amendment rights against the Government's need to elicit intelligence information for purposes of national security.

The reasoning employed to object to H.R. 9781, Section 2(5), also compels us to object to H.R. 13825. This bill was proposed to prevent abusive practices and procedures by the Government when engaging in investigation and law enforcement activities utilizing electronic surveillance techniques. These abusive practices and procedures were declared to be especially excessive in instances involving security. To further this end, H.R. 13825 recommends amending Section 2511(3) to limit its provisions solely to the protection of the national security against foreign powers and agents.

The policy of the President and the Attorney General relating to national security wiretaps was recently set forth by former Attorney General Richardson. In reply to questions raised during the recent hearings on the confirma-

tion of Henry Kissinger as Secretary of State, Attorney General Elliot Richardson sent a letter to the Senate Foreign Relations Committee outlining the Justice Department's policy in light of *United States* v. *U.S. District Court*, 407 U.S. 297, 11 Cr. L. 3131, (1972), and pending litigation on the subject.

The full text of Attorney General Richardson's letter to Senator J. W. Fulbright (D. Ark.) follows:

"SEPTEMBER 12, 1973.

"DEAR MR. CHAIRMAN: During the confirmation hearing of Dr. Kissinger, a question was raised as to this Administration's position concerning the power of the Executive to conduct electronic surveillance without warrant in the national security field. Dr. Kissinger said that he would try to elicit a statement for the record that would clarify our general policy on this matter.

"I believe that there will continue to be situations which justify the conduct of electronic surveillance for the purpose of national security. This surveillance is carried out to meet the obligations of the President as both Commander-in-Chief and as the Nation's instrument for foreign affairs. I will continue to attempt to ensure that a genuine national security interest is, in fact, involved whenever we invoke this power and that we operate within the limits set by Congress and the courts.

"The Department of Justice scrupulously observes the law as interpreted by the courts. There may be questions as to what certain decisions mean and whether surveillance, such as that discussed by the committee, has been affected by later court decision. These and other issues are before the courts now and we expect any ambiguities to be settled within the normal judicial process. The policy statement that follows therefore refers to procedures for any surveillance that may be carried out at present.

"A year ago in the *Keith* case (407 U.S. 297, 11 Cr. L. 3131), the Supreme Court ruled unanimously that the Government may not carry on electronic surveillance in domestic security operations, as opposed to foreign intelligence operations, without first obtaining a judicial warrant. The Court pointed out that it was condemning warrantless electronic surveillance carried out in domestic security cases directed at a "domestic organization (whether formally or informally constituted) composed of citizens of the United States and which has no significant connection with a foreign power, its agents or agencies." The *Keith* decision necessarily is Departmental policy and is being followed.

"Although the *Keith* case did not address warrantless national security electronic surveillance, to date, the lower courts which have addressed this problem have agreed with the contention of this Department that a judicial warrant is not a necessary requirement for the Government's use of electronic surveillance to obtain foreign intelligence or foreign policy information necessary for the protection of national security. *E.G., United States* v. *Clay*, 430 F. 2d 165 (5th Cir. 1970), reversed on other grounds, 403 U.S. 698 (1971); *United States* v. *Brown*, 317 F. Supp. 531 (E.D. La., 1970), affirmed, No. 72-2881 (5th Cir., Aug. 22, 1973); *United States* v. *Smith*, 321 F. Supp. 424 (C.D. Calif. 1971); *Zweibon* v. *Mitchell*, 42 U.S. L. Week 2054 (1973). Pending a decision on this issue by the Supreme Court I believe that we are justified in relying on the case law as it is being developed in the lower courts to conduct national security electronic surveillance, without warrant, in a limited number of cautiously and meticulously reviewed instances.

"When Congress enacted legislation in 1968 requiring a judicial warrant for the use of electronic surveillance in investigations of violations of certain criminal laws, it made clear that it did not intend to add or subtract from whatever measure of constitutional power the President may have to use electronic surveillance in the national security field. However, as a guide, it set forth a number of purposes, divided between the domestic and foreign aspects of national security, that it understood to be proper for the exercise of Presidential power. The *Keith* decision subsequently held that this power could not, in the absence of a warrant, be exercised for the domestic security purposes mentioned by Congress. However, as a matter of policy, I shall keep in mind the contours of the President's power suggested by Congress in the 1968 law as it relates to foreign intelligence. In general, before I approve

any new application for surveillance without a warrant, I must be convinced that it is necessary (1) to protect the nation against actual or potential attack of other hostile acts of a foreign power; (2) to obtain foreign intelligence information deemed essential to the security of the United States. or (3) to protect national security information against foreign intelligence activities. 18 U.S.C. 2511(3).

"As the Supreme Court itself observed in Keith, it may well be difficult to distinguish between "domestic" and "foreign" unlawful activities directed against the United States where there are relationships in varying degrees between domestic groups or organizations and foreign powers, or their agents. All I can say is that, as the applications are presented to me, I will, together with my staff, try scrupulously to follow the guidance and instruction given to us by Congress and the courts, bearing in mind the importance of balancing individual privacy with the needs of national security."

Therefore, the proposal in H.R. 13825 deleting the second sentence of Section 2511(3) is needless, as the former Attorney General's statement, adhering to *United States* v. *United States District Court*, 407 U.S. 297 (1972), indicates that the Department is scrupulously observing the procedures laid out by the Supreme Court.

In addition, the proposal in H.R. 13825 limiting the admissibility of contents or evidence of intercepted communications to civil proceedings against foreign agents is also objectionable to us. As we feel that wire and oral communications may be intercepted in the name of national security, both against foreign and domestic subversion, subject to the *Keith* decision.

Further, we feel that Section 2515 of Title 18 adequately covers the situation which this proposal seeks to amend. Section 2515 states that ". . . no part of the contents of such [intercepted] communication and no evidence derived therefrom may be received in evidence . . . if the disclosure of that information would be in violation of *this chapter*." (Emphasis supplied). This statute obviously covers the suppression of intercepted evidence where the interception procedure and authorization is pursued contrary to Sections 2516 and 2518. It further covers the procedures for national security surveillances, under Section 2511(3), and *United States* v. *United States District Court*, 407 U.S. 297 (1972). These reasons compel us to object to the enactment of the proposal in H.R. 13825 limiting the admissibility of national security surveillance to civil proceedings.

H.R. 13825 also proposes to supplement the present Sections 2516 and 2518, by adding the new Sections 2516A and 2518A. These recommended amendments are consistent with the bill's earlier proposal to limit the provisions of Section 2511(3) to national security surveillances solely against foreign agents and powers. We understood that the intent of this bill is to make foreign intelligence surveillances by electronic means obtain prior court approval before utilization.

Since the Supreme Court's decision in *United States* v. *United States District Court*, 407 U.S. 297 (1972), this Department would employ an appropriate prior warrant procedure where security surveillances were to be applied for in the name of domestic security. It is our view that neither this decision nor Section 2511(3) requires a warrant, or judicial approval, before surveillance may be undertaken where the national security is threatened by or on behalf of foreign powers. Former Attorney General Richardson's letter to Senator Fulbright points out that several lower Federal courts and courts of appeals also adhere to this belief. Further, the Executive power "to preserve, protect and defend the Constitution" in Article II, Section 1, also supports our view.

Thus, we cannot support the proposal in H.R. 13825 to establish guidelines for the authorization of and procedures for interceptions of wire and oral communications relating to national security cases against foreign powers. We cannot help but feel that these amendments would contravene the President's power under the Constitution by requiring a prior judicial determination of probable cause to believe certain enumerated crimes have been or are about to be committed by foreign agents thereby endangering the national security. Unless, and until, we receive a judicial construction of the Executive

power in Article II, Section 1, that requires prior judicial approval for electronic surveillances in national security cases against foreign powers, we do not believe that Congress should enact these proposals. For this reason, we object to their passage.

In sum, I want to thank you for the opportunity to express the views of the Department of Justice on pending legislation relating to the subject of wiretapping and electronic surveillance. We do not feel that these proposals will further nor support the present Title III of the Omnibus Crime Control and Safe Streets Act of 1968, nor are they consistent with the expressions of the various Federal courts. Consequently, we recommend against the passage of H.R. 1597, H.R. 9667, H.R. 9698, H.R. 9781, H.R. 9815, H.R. 9949, H.R. 11629, H.R. 11838, and H.R. 13825.

Mr. KASTENMEIER. Thank you, Mr. Petersen and Mr. Maroney.

The Chair would next like to call, representing the Department of Defense, the Deputy Assistant Secretary of Defense for Administration, Mr. David O. Cooke. Prior to joining the Department, Mr. Cooke served as a career naval officer, retiring with the rank of captain. We are very pleased to have Mr. Cooke and his assistants here this morning. I know that at least one of your group may have time problems, and we will try to expedite your testimony.

TESTIMONY OF HON. DAVID O. COOKE, DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR ADMINISTRATION, DEPARTMENT OF DEFENSE, ACCOMPANIED BY JOSEPH J. LIEBLING, DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR SECURITY; AND ROBERT T. ANDREWS, ASSISTANT GENERAL COUNSEL

Mr. COOKE. Thank you, Mr. Chairman. May I introduce my two colleagues. On my right, is Mr. Joseph Liebling, Deputy Assistant Secretary of Defense for Security Policy and on my left, Mr. Robert Andrews, Assistant General Counsel in the Department of Defense.

Mr. Chairman and members of the committee, I am here in response to your invitation to the Secretary of Defense to furnish information in connection with your inquiry into changes to title III of the Omnibus Crime Control and Safe Streets Act of 1968, and to provide information relating to the policies and procedures by which wiretapping and electronic surveillance are authorized and controlled within the Department of Defense.

For management purposes, the Department has placed wiretapping and electronic surveillance activities into two separate categories.

Department policies and procedures which limit the use of telephone monitoring and control the use of information obtained by third parties, are set forth in Department of Defense Directive 4640.1, "Telephone Monitoring." DOD policies which restrict the use of wiretapping and eavesdropping during the conduct of investigations for law enforcement purposes are published in DOD Directive 5200.24, "Telephone Interception and Eavesdropping." Both of these directives apply to the United States, the Commonwealth of Puerto Rico and U.S. territories. They do not apply elsewhere overseas, nor are they applicable to our foreign intelligence collection activities. Copies of the two directives were provided to your committee last week.

First, I would like to discuss telephone monitoring which is administrative rather than investigative in purpose. There are four classes of telephone monitoring. They are:

1. OFFICE TELEPHONE

Listening to or recording office telephone communications by use of mechanical or electronic devices or recording by written means, for the purpose of obtaining an exact reproduction or a summary of the substance of the telephone conversation and with the consent of all parties.

2. COMMAND CENTER COMMUNICATIONS

Listening to or recording telephone communication in DOD command centers for the purpose of obtaining a record of conversations, or parts thereof, for command and control purposes.

3. COMMUNICATIONS SECURITY

Listening to or recording of the transmission of official defense information over DOD-owed or leased telephone communication, by any means, for the purpose of determining whether such information is being properly protected in the interest of national security. Notice of this action is given to users that these systems are subject to communications security monitoring at all times.

4. COMMUNICATIONS MANAGEMENT

Listening to or recording telephone communications on DOD-dedicated systems or the common-user systems of the Defense communication system, by any means, not for the contents but for the purpose of determining whether the systems are functioning properly for official purposes. Almost every phone company has a counterpart activity.

The first class of telephone monitoring is one in which you are all familiar, called office monitoring. With the use of either a recorder equipped with "beeper" or with a stenographer, it requires the advance consent of all parties to the conversation. Office telephone monitoring, in such cases, is a valuable management tool to reflect the exact nature of agreements and understanding achieved by telephone. One of the parties to the conversation may be outside the DOD but again let me emphasize that all parties concerned must consent to office telephone monitoring.

The other three classes of telephone monitoring are largely internal. That is, they are directed to the manner in which DOD military and civilian personnel use telephones which are part of DOD communications systems.

Telephone monitoring in command centers, for communications security and for communications management purposes, does not require express consent in each case. The purpose of command center monitoring is to obtain accurate records for command and control purposes of official calls to a command center. Examples of the command centers are the National Military Command Center, its alter-

nate, the Airborne Command Post, the North American Air Defense Command Post, the Military Services Operations Centers in Washington, the Military and Security Police Operations Centers, Fire and Rescue Control Centers and Air Traffic Control Centers.

DOD monitoring for these Centers closely compares with the recordings made by the Federal Aviation Agency in its many air traffic control centers. Similarly, most police, fire, and rescue control centers in our large cities and counties monitor incident reports and requests for assistance to insure accuracy and for record purposes. Furthermore, command centers are able to record messages to be rebroadcast to subordinate and lateral units.

DOD Directive 4640.1 requires for each center specific regulations be published prior to the initial operation of the recording equipment. The existence of such monitoring, however, is required by DOD Directive 4640.1 to be so widely and expressly publicized throughout DOD and its components as to amount to constructive consent.

Our authority for this class of monitoring equipment and its use stems from communications common carrier tariffs which have been approved by the Federal Communications Commission. This class of monitoring is provided for in DOD Directive 4640.1, which I mentioned earlier.

Communications security monitoring—COMSEC monitoring—is the third class of administrative telephone monitoring which is used, albeit rarely, on Department of Defense telephone circuits. The purpose of COMSEC monitoring is to provide a basis for analysis to ensure that classified information is not discussed on unsecure telephones.

This monitoring may only be conducted when authorized by the commander or DOD official in charge of an installation or activity or his superior. Let me stress that security organizations organized and equipped to perform communications security monitoring are not authorized to monitor communications systems on their own initiative. Communications security monitoring is employed infrequently. Less than one percent of our telephones are monitored for security in any given year.

The lines selected for security monitoring consist mainly of those serving command posts, major operational headquarters, war rooms, and field exercises both in the United States and overseas.

Let me emphasize that the purposes of COMSEC monitoring are to advise commanders on actual or possible security compromises and improve the security protection of telephone communications.

DOD Directive 4640.1 expressly states that the information obtained as a result of telephone communications security monitoring shall not be authorized for law enforcement purposes unless the General Counsel authorizes an exception in a specific case.

The last class of administrative telephone monitoring is communications management monitoring, often called service observation. Service observation is conducted largely by computer analysis and pay count methods rather than by actual listening to telephone conversations in progress.

It is a tool used to determine if telephone systems are functioning properly, not with the contents of conversations, but with such things

as the precedence and number of calls, their duration, response to signals, number of busy signals for a given time period, total load on a system in numbers and duration of calls, etc.

The purpose of administrative telephone monitoring previously described, is distinctly different from the purpose of wiretapping or eavesdropping. Telephone monitoring is to accurately preserve records of conversations as in command centers, or to analyze a total system for adherence to protection of classified information as in COMSEC monitoring.

Wiretapping and eavesdropping are used for the purpose of criminal investigations.

Let me now turn to the Department's policies and procedures for telephone interception and eavesdropping techniques used in investigating criminal cases. DOD defines these terms exactly as they are defined in title III of Public Law 90–351:

Telephone Interception—wiretapping. The use of electronic, mechanical, or other devices to intercept a wire communication for the purpose of obtaining information as part of a criminal investigation.

Eavesdropping—Electronic Surveillance. The use of electronic, mechanical, or other devices to intercept an oral communication for the purpose of obtaining information as part of a criminal investigation.

DOD Directive 5200.24 authorizes, under controlled circumstances, the use of telephone interception—or wiretapping— and nontelephonic electronic surveillance—eavesdropping—by DOD criminal and investigative agencies when there are reasonable grounds to believe that:

1. A criminal offense concerning the national security is involved; or 2. a felony has been or is about to be committed; or 3. telephone calls involved obscenity, harassment, extortion, bribery, or threat of bodily harm have been made to a subscriber-user on a military base.

Wiretap and eavesdrop operations conducted by DOD are in full compliance with the policies and requirements established by the Attorney General and issued pursuant to 18 U.S. Code, chapter 119.

Let me stress most strongly that the DOD is not in the business of conducting electronic surveillance of civilians not affiliated with the Department. DOD Directive 5200.27 expressly forbids such practices except in narrowly defined circumstances. In other words, the wiretaps or eavesdrops DOD conducts are employed only in cases involving military or, in extremely rare cases, DOD civilian personnel provided the FBI has yielded jurisdiction.

The procedures I am about to describe are those instituted by the Attorney General for consensual wiretaps and eavesdrops. That is, at least one party has consented. All non-consensual cases, should any arise, must be referred to the Attorney General. None have arisen in DOD since the passage of P.L. 90–351 in 1968.

Under the Attorney General's procedures and the provisions of DOD 5200.24, consensual wiretaps may be authorized by heads of DOD components or their designees for the investigation of criminal cases and harassing telephone calls. DOD components have issued regulations setting forth procedures and controls for these authorizations.

The Attorney General has adopted stricter rules in the case of eavesdrops. For consensual eavesdropping of nontelephone conversations, prior approval normally must be obtained from the Department of Justice. Again, DOD Directive 5200.24 provides first that the head of the DOD component concerned, or his designee, must approve the proposed eavesdrop. Then it must be approved by the DASD/A before it is sent to the Attorney General requesting his approval. Attorney General regulations provide for emergency monitoring in advance of his approval to prevent the immient loss of essential evidence. In such cases, a full report of justification must be provided to him.

Each request for approval of proposed wiretapping or eavesdroppnig must contain a detailed statement as to the crimes and persons involved and a statement that the consent of one party has been obtained with his identity. All approvals are limited to 30 days, as are any renewals.

DOD Directive 5200.24 provides careful safeguards both as to the integrity of equipment and any information obtained by their use.

The wiretapping and eavesdropping devices are carefully accounted for and stored under secure conditions by the investigative agencies of our Military Departments. Both categories of electronic devices are only authorized for use in approved cases under the supervision of experienced aegnts who have been instructed in the legal and private rights aspects of their use.

With respect to the information that might be received by wiretapping or eavesdropping activities, DOD Directive 5200.24 requires that it be stored in appropriate investigative files at a central location; that the information so stored is always identified, when used for any purpose, as information which was obtained by wiretapping or eavesdropping; that access to information so stored is strictly controlled and recorded and that this information shall not be disclosed outside of the Department of Defense unless the head of the DOD Component concerned determines that disclosure is essential to governmental operations.

Finally, the Directive requires quarterly reports to the Secretary of Defense concerning the employment of wiretaps and eavesdrops, including those conducted in areas of the world where the substantive provisions of the Directive do not apply. We also have an annual summary and electronic equipment report to make to the Attorney General.

In recent years, wiretapping has shown an increase in cases involving drugs and telephonic bomb threats or other harassing calls. Eavesdropping activities have shown a marked increase over the last several years attributable almost completely to the narcotics and drug problem.

Consensual intercepts, particularly eavesdrops, have contributed significantly to our success in drug cases. However, because of the type and short duration of the calls, we have been only moderately successful in identifying the callers in bomb threats and similar cases. Both wiretapping and eavesdropping are essential elements in the DOD Law enforcement program.

Department of Defense programs and activities under DOD 5200.24 which have been discussed would be affected adversely by

pending legislation relating to wiretapping and electronic surveillance. In particular H.R. 9698 would prohibit the interception of certain communications unless all parties to the intercepted communication consent. The effect of H.R. 9698 would be to eliminate the use of wiretaps or eavesdrops in any criminal case. Obviously, none of the narcotic and drug cases which the Military Services have investigated successfully on the basis of consensual intercepts undertaken in accord with the present law would have been possible if the prior consent of each of the parties had been a necessity.

The bill, in my judgment, would not impact on our administrative telephone monitoring procedures which are now based on actual or implied consent of all parties.

Mr. Chairman, I have appreciated the opportunity you have afforded the DOD to describe its policies and practices in the area of electronic surveillance. We realize that this is an area of balancing the rights of the individual on one hand and the legitimate needs of an organized society on the other. We believe our directives are not only in full compliance with the law and the Attorney General's regulation but also have achieved that balance.

Mr. Drinan [presiding]. Thank you very much, Mr. Cooke.

In the absence of the chairman temporarily, I will begin the questioning.

On page 1 of your statement you indicate that the Department of Defense (DOD) Directive which restricts the use of wiretapping does not apply overseas. Does that mean that the DOD conducts warrantless national security wiretapping in the United States, as well as overseas, and to what extent, if you do that, is that approved by the Attorney General?

Mr. Cooke. Mr. Drinan, the Department of Defense does not conduct warrantless wiretapping in the United States, although the Directive does provide that in cases we would go to the Attorney General, as we do in the case of consensual eavesdropping exempted, as you know, from the provision of title III. But, since the law has been passed, we have had no occasion in the United States to go to the Attorney General for a request for warrantless wiretap.

Mr. Drinan. What about overseas?

Mr. Cooke. Overseas, the Department of Defense Directive does not apply. By its terms, it is limited, as I indicated, to the United States, the Commonwealth of Puerto Rico and the U.S. territory.

Mr. Drinan. Does it apply to American citizens overseas?

Mr. Cooke. It does not.

Mr. Drinan. Therefore, was the wiretapping and surveillance of McGovern campaing workers in Germany in 1972 conducted in this manner, pursuant to an exception, if you will, or without the DOD Directive?

Mr. Cooke. Mr. Drinan, I am aware it goes back to July and August of 1973, and there appeared to be in the press a number of stories concerning alleged Army surveillance of U.S. citizens, foreign nationals and organizations, both foreign and domestic, based in the Federal Republic of Germany and in Berlin. The Army looked into this matter, and I can only say at this time that, as you know, in February 1974, a complaint was filed in the

U. S. District Court for the District of Columbia against the Secretary of Defense and the Secretary of the Army and the entire chain of the Army Command responsible for intelligence activities in Europe concerning this alleged surveillance. The case is entitled, *Berlin Democratic Club et al.* v. *Schlesinger et al.* It alleges charges of illegal wiretapping, interception of mail, infiltration and penetration of meetings and maintenance of intelligence dossiers. It would be highly inappropriate for me to comment on a case now in litigation, and on the advice of the Department of Justice I would prefer not to discuss the facts involved in the lawsuit. I can add that the counter-intelligence measures that were adopted by the Army in Europe have been conducted in accordance with our international obligations, the laws of the host nation in which troops are located. We are confident of the issue as presented in the pending litigation will be resolved in the government's favor.

Mr. DRINAN. Well, Mr. Cooke, would you answer my question? If these were conducted, I assume there is some record of it, and would that record be included in the quarterly and annual reports to the Secretary and to the Attorney General?

Mr. COOKE. The record, as I said, would not be governed by the provisions of our Directives because they are overseas. We would have a quarterly report of eavesdrops or telephone interceptions in areas outside of the purview of the directives.

Mr. DRINAN. Where are they contained?

Mr. COOKE. The quarterly reports are sent into the Office of the Secretary of Defense.

Mr. DRINAN. Could we have that quarterly report? You mention on page 10 that you do have these quarterly reports on warrantless national security surveillance. Would you furnish us with one or more, and particularly with the one in which the wiretapping or alleged wiretapping and surveillance of the McGovern campaign workers is noted?

Mr. COOKE. Mr. Drinan, I have stated that the Department of Defense has no record of engaging in warrantless surveillance within the meaning of title III of the law, because, as you know, the provisions of the law are limited, as are the provisions of our directives to the United States, to the Commonwealth of Puerto Rico and the United States territories and possesions. So, to use the term warrantless activities, or warrentless wiretaps overseas, I think is not the proper use of the term.

Mr. DRINAN. Mr. Cooke, may I rephrase and clarify it.

On page 10 you state:

> **Finally, the Directive requires quarterly reports to the Secretary of Defense concerning the employment of wiretaps and eavesdrops, including those conducted in areas of the world where the substantive provisions of the Directive do not apply.**

Consequently, I am asking therefore that quarterly or annual reports, or both, which contain a record of all wiretaps and eavesdrops, including those conducted in areas of the world where the directive does not apply, be supplied.

Mr. COOKE. Mr. Drinan, we will attempt to furnish you that. The record of the wiretaps and eavesdrops conducted overseas of neces-

sity in many cases contain information classified under the provisions of the Executive Order 11652. I can give you totals right now if you are interested.

Mr. DRINAN. We are very interested. Give us the totals.

Mr. COOKE. In calendar year 1973, in the Continental United States, and I will go through those first, if I may, the number of requests for approval of consensual or oral electronic surveillance, where we sent the requests to the Attorney General and got his approval, 48. Now, bear in mind these are not warrantless because these are the consent of one party. And under the provisions of 2511, section 2(C) and (D) of title III consensual taps are expressly excluded from provisions of title III. But, the Attorney General has seen fit to impose higher standards than the law and I think quite properly.

The number of electronic surveillance cases reported by DOD components outside of the United States, the Commonwealth and territories during calendar year 1973 was a total of 42, sir. In the case of telephone taps, electronic or wiretapping, again consensual, but where the Attorney General has not said he demands advance approval, in the United States these consensual taps in 1973 totaled 55, overseas, and in calendar year 1973, 27.

Mr. DRINAN. Would you have those also, sir, for 1972?

Mr. COOKE. As a matter of fact I do, sir. Let me run through them.

Mr. DRINAN. If you would.

Mr. COOKE. I do not think—let me preface this by saying the Attorney General's memorandum about consensual taps dated October 16, 1972, and issued December 1, 1972. We only show one request and that was approved, but not used. My figures started essentially with 73, and I have them for the first quarter of 1974.

Mr. DRINAN. Mr. Cooke, would you explain again the exact ruling of the Attorney General in October of 1972?

Mr. COOKE. The Attorney General in October 1972, in a memorandum issued to the heads of Executive Departments and Agencies, subject, "Monitoring Private Conversations with the Consent of a Party," expressly stated that this memorandum does not restrict any form of monitoring where all parties to the conversation consent, nor does it affect his existing instructions on the related matter of electronic surveillance without the consent of any party to a conversation. This memorandum established procedures whereby in the case of a—and I am now quoting from page 5 of the memorandum, and the administrative regulation concerning consensual monitoring of conversations, the Attorney General observed, "it is clear that such montitoring is Constitutionally and statutorily permissible, and, therefore, that it may be conducted without a judicial warrant." Bear in mind I am talking about consensual taps or surveillance which the provisions of 2511 of title XVIII, section 2(C) and (D) expressly state or exclude from the provisions of that section. These are interceptions for one of the parties to the communication has given prior consent to such interception, and this is the subject of the Attorney General's memo. The Attorney General provided that for conversations other than telephone conversations:

. . . all Federal departments and agencies shall, except in the exigent circumstances, as discussed below, obtain the advanced authorization of the Attorney General or his designated Assistant Attorney General before using any mechanical or electronic device to overhear and transmit or record . . ."

Mr. DRINAN. Mr. Cooke, in view of that, assuming that the McGovern campaign workers would have been tapped, prior to October 1972, what record would the DOD have of the alleged wiretap?

Mr. COOKE. Wiretapping? Mr. Drinan, the information we have had in the pending litigation that I discussed before was that it was in 1973 that these incidents took place, not 1972.

But, to return to the Attorney General's memorandum with respect to telephone conversations, again where one party has consented, the Attorney General says that because the transmission of the participants' conversations through a complex and far-flung network of wires, the common use of multiparty lines and extension telephones, and the possibility of an unseen participant permitting another person to listen have long been considered not to justify the same assumptions as that of a private, face-to-face conversation. Accordingly, the current practice of charging each department and agency with a control of such consensual monitoring by its agents will continue. That is the provisions that are embodied in the directive which we have furnished you, sir.

Mr. DRINAN. Going back to this question, Mr. Cooke, of consensual, and apparently implied consent, it is construed by DOD to mean constructive consent. Let me just give a hypothetical. If somebody is suspected of selling or using hard drugs, who is the consensual person in a wiretap conversation? Would it be his superior officer, or who would in this case be deemed to have given consent?

Mr. COOKE. Mr. Drinan, I talked about implied consent only with respect to the four classes administered, or three classes of administrative telephone monitoring which were not for the purpose of criminal investigations. This is communications security, the command and control or operations center and traffic management, which really does not involve listening. But, in the case you cited we are talking about a law enforcement or a criminal investigation, where one of the two parties to that phone call has consented to wiretap, or one of the parties involved in the telephone surveillance has.

Mr. DRINAN. From the normal course of events, how would this person have consented? Is he an informer or a law enforcement official himself?

Mr. COOKE. In the normal course of our investigation in a drug case, and that is mainly where they arise here, we would be using an informer, a military man, or possibly one of the actual agents of one of our criminal investigations, who have succeeded in contacting the suspect.

Mr. DRINAN. Has there been any challenge to that implied consent? You state that certain monitoring is considered to be given with the constructive consent of DOD personnel. Is there any statutory or judicial authority for the concept?

Mr. COOKE. I think the statement is essentially with respect to the communications security monitoring that I described as the third of the three classes. There are several things. One is issued pursuant to

the National Security Act of 1947, as amended where there is a National Scurity Council Communications Security Directive, which among other things, provides that the heads of individual departments and agencies, with the responsibility for executing all measures required to assure the security of the Federal communications, and we are trying to protect an unsecure line, and the use of, or casual discussion of classified information on an unsecured line, and I would also observe this is done essentially in field exercise, in command posts and the like. It is less than one percent of our phones at any time. I mean, during the year being subject to this monitoring. Our directive provides for express prior notice measures to all subscribers. And let me read that provision, if I may.

I am quoting now from DOD Directive 4640.1, paragraph 5(C)(2):

Such regulations referring to COMSEC monitoring shall be widely distributed in all elements of the Department of Defense concerned, and shall contain the following specific statements as a minimum for information and guidance of users of Department of Defense Telephone Communications Systems. The Communications Systems are, one, providing for transmission of official government information only; and, two, that they are subject to communications security monitoring at all times.

Mr. DRINAN. Mr. Cooke, I have that regulation here.

Mr. COOKE. I am quoting from page 44.

Mr. DRINAN. Yes. I have it right here. But, I go back to my original question. Is there any authorization from Congress or the courts for this very broad understanding of constructive consent? Certainly this could not be done in General Motors, it could not be done in the Department of Labor with civilians. Is there any statutory or judicial authority for this concept.

Mr. COOKE. First of all, I think there is recognition of the requirement of this concept in 25 U.S. Code Title XVIII, 2511, which states in subsection (3) that nothing contained in this chapter shall limit the constitutional power of the President to protect national security information against foreign intelligence activities.

Mr. DRINAN. Do you really think that that justifies it?

Mr. COOKE. I think this justifies the communications security monitoring, and I will also add again that—and again I quote from our directive that the users have been notified, as outlined in paragraph 2(A) above, and the DOD communications system shall constitute consent to the communications security monitoring.

Mr. DRINAN. Do you think a statute enacted by the Congress could protect the right of privacy of people in the military without any really severe or any damage to security?

Mr. COOKE. No, I do not, and we are concerned that on an unsecure phone, and it is a natural tendency because of the ease of talking on a phone, there are occasions where information, properly classified to protect national security, has been discussed on unsecured lines. And, believe me, we are targeted both here in the United States and monitored overseas by people who can listen to us. Again, let me emphasize the purpose of this is not law enforcement. The purpose of this is to advise commanders on actual or post-security compromises, and to improve the security protection of telephone communications.

The directive expressly states that information obtained as a result of telephone communications security monitoring shall not be used for law enforcement purposes.

Now, it is true that it says any proposed exceptions shall be submitted by the head of the DOD component concerned to the General Counsel for consideration. And I will state categorically we have never had a request for such an exception.

Mr. DRINAN. Thank you, Mr. Cooke.

I yield at this time to my colleague from New York, Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman.

Mr. Cooke, I think you just answered the question I was going to ask you and that was in regard to COMSEC information being authorized for law enforcement purposes. And you just said that you never had such a request.

Mr. COOKE. We have never had although the directive does contemplate that possibility.

Mr. SMITH. When you talk about that in connection with law enforcement, are you talking about military law enforcement or any kind of law enforcement purposes?

Mr. Cooke. We are talking both, but essentially as you know, the Uniform Code of Military Justice, in its penal provision, which applies to all of our military personnel, in large measure repeats most of the offenses of title XVIII, generally. But, in our criminal law enforcement investigations in the United States, we are focusing almost exclusively on military personnel, very rarely on a civilian employee of the Department, and then only in terms of the delimitations agreement between the Bureau and the Department of Defense.

Mr. SMITH. If I understood your statement, you are prohibited by regulations, if not by law, from monitoring civilians who do not have any connection with the military?

Mr. COOKE. Yes, we do. DOD Directive 5200.27 has a prohibition. We can furnish a copy of it. It expressly eliminates electronic or other surveillance except under some very narrowly, carefully defined circumstances, where it constitutes an immediate threat to personnel or property. But, there is an express prohibition in the directive, sir.

Mr. SMITH. And the civilians that might be monitored if I understood your statement correctly, who are employed by the Military Service, you may monitor them only if the FBI has in advance waived their right?

Mr. COOKE. If we are talking about criminal investigations, of our civilian employees, of course.

Mr. SMITH. I can understand that. But, in criminal investigations?

Mr. COOKE. Yes. We had, as you know, a De-limitations Agreement with the Bureau as to who investigates many of the offenses, as I indicated, for military personnel, which could be subject to either trial by court-marital or trial in a local or Federal court.

Mr. SMITH. Let me ask you a possible for instance. For instance, if there were a civilian employed by the military, who was selling drugs as a moonlighter at home, this would probably be pursued by the FBI?

Mr. COOKE. I think so or local authorities, yes, sir.

Mr. SMITH. But if you were selling drugs on the base, a military base, it probably would be pursued by the military?

Mr. COOKE. Pursued, perhaps investigated would be the better word because we would have made arrangements for jurisdiction and for a criminal trial by civil court.

Mr. SMITH. I will accept that amendment. Thank you very much.

Mr. DRINAN. Thank you, Mr. Smith. I yield to our counsel for some questions.

Mr. LEHMAN. Mr. Cooke, I wonder if you could clarify something you mentioned a little earlier, and that is, did you mean to indicate that you would supply the committee with the quarterly report to the Secretary of Defense and the annual summary to the Attorney General?

Mr. COOKE. I indicated we would supply you the numerical tabular data for it. I would want to go back and check as to the exact details of factual information, as to the facts involved in such case. I think we can do that, but recognizing that some cases would have the information classified, and in other cases, there are other provisions of the Freedom of Information Act, other than classification which would impede public disclosure.

Mr. DRINAN. Well, Mr. Cooke, I would take it that is the sense of the committee, that the information would be very helpful, and we hereby request it. We, obviously, will keep classified information classified.

Mr. COOKE. We will be back in touch on that.

Mr. DRINAN. OK.

Mr. LEHMAN. Another question.

You supplied the committee, in response to the Chairman's letter to the Secretary of Defense, with a copy of DOD Directive 5200.24 dated August 17, 1967.

[The exchange of correspondence between the Chairman and the Department of Defense follows:]

HOUSE OF REPRESENTATIVES, U.S.,
COMMITTEE ON THE JUDICIARY,
Washington, D.C., April 10, 1974.

Hon. JAMES R. SCHLESINGER,
Secretary of Defense,
Department of Defense,
Washington, D.C.

MY DEAR MR. SECRETARY: The Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the House Judiciary Committee has scheduled hearings on April 24, 26, and 29 on wiretapping and electronic surveillance. In order that the Subcommittee may be adequately informed about the surveillance practices of the Department of Defense, I would appreciate your replying to the following questions by close of business, April 18.

1. Does the Department permit monitoring of incoming or outgoing telephone calls by third persons: a. with the consent and knowledge of both parties to the call? b. With the consent and knowledge of only one party to the call? c. Without the consent and knowledge of either party to the call?

2. Does the Department permit monitoring of telephone calls betwen telephones within the Department under the circumstances described in a, b, and c above?

3. Does the Department have any rules or regulations covering telephone monitoring, recording, and surveillance? If so, please provide two copies.

4. Does the Department permit the use of wiretapping or electronic surveillance as an investigative technique by military police agencies invstigating suspected criminal violations?

5. Does the Department ever utilize non telephonic electronic surveillance devices of any kind? If so, of what type and for what purposes?

6. Does the Department possess telephonic recording devices? If so, how many, and is a beeper or other warning device required to warn parties to the call of the recording?

If you or your staff have any questions regarding this request please call Bruce Lehman, Subcommittee Counsel, 225-3926.

Sincerely yours,

ROBERT W. KASTENMEIER,
Chairman, Subcommittee on Courts, Civil Liberties and the Administration of Justice.

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE,
Washington, D.C., April 19, 1974.

HON. ROBERT W. KASTENMEIER,
Chairman, Subcommittee on Courts, Civil Liberties, and the Administration of Justice, Committee on the Judiciary, House of Representatives, Washington, D.C.

DEAR MR. CHAIRMAN: Your letter to Secretary of Defense Schlesinger of April 10, 1974, regarding wiretapping and electronic surveillance has been referred to me for reply.

The Department of Defense separates wiretapping and electronic surveillance into two categories:

1. Telephone monitoring.

2. Telephone interception (wiretapping) and eavesdropping (electronic surveillance) employed during the conduct of investigations for law enforcement purposes in the United States.

Telephone monitoring in turn is divided into four classes:

1. *Office telephone*—Listening to or recording office telephone communications by use of mechanical or electronic devices or recording by written means, for th purpose of obtaining an exact reproduction or a summary of the substance of the telephone conversation.

2. *Command center communications.*—Listening to or recording telephone communications in DoD command centers for the purpose of obtaining a record of conversations, or parts thereof, for command purposes.

3. *Communications security.*—Listening to or recording the transmission of official defense information over DoD owned or leased telephone communications, by any means, for the purpose of determining whether such information is being properly protected in the interest of national security.

4. *Communications management.*—Listening to or recording telephone communications on DoD-dedicated systems or the common-user systems of the Defense Communications System, by any means, for the purpose of determining whether the systems are functioning properly or being used for other than official purposes.

The following answers are keyed to your questions which have been included verbatim for ease of reference.

Question 1. Does the Department permit monitoring of incoming or outgoing telephone calls by third persons: a. with the consent and knowledge of both parties to the call?

Answer. (1) Office telephone monitoring is permitted only with the consent of all parties to the call.

(2) Command center communications recording is authorized for command and communications purposes pursuant to regulations issued by the head of the DoD component concerned in command centers such as the National Military Command Center in the Pentagon.

(3) Communications security monitoring is undertaken only as specified in regulations issued by the head of the DoD component concerned to provide

for analysis and to determine the degree of security being afforded telephone transmissions.

(4) Communications management monitoring is undertaken only to provide material for analyses within DoD to determine the operational efficiency and proper use of DoD communications systems.

Question 1b. With the consent and knowledge of only one party to the call?

Answer. (1) Office telephone monitoring is not authorized unless the consent of all parties is obtained.

(2) The other three classes of telephone monitoring are permitted as described in the replies to question 1.a. above.

Question 1c. Without the consent and knowledge of either party to the call?

Answer. (1) No. See answer to question 1.a.(1) above.

(2) DoD directives and implementing regulations relating to the other three classes of telephone monitoring prescribe wide advance notice of such monitoring to users, tantamount to consent.

Question 2. Does the Department permit monitoring of telephone calls between telephones within the Department under the circumstances described in a, b, and c above?

Answer. The answers to question 1 also apply to telephone calls within the Department of Defense.

Question 3. Does the Department have any rules or regulations covering telephone monitoring, recording, and surveillance? If so, please provide two copies.

Answer. DoD policy with respect to telephone monitoring is contained in DoD Directive 4640.1 DoD policy with respect to telephone interception and eavesdropping is contained in DoD Directive 5200.24. Copies of both directives are attached.

Question 4. Does the Department permit the use of wiretapping or electronic surveillance as an investigative technique by military police agencies investigating suspected criminal violations?

Answer. Yes. Wiretapping and eavesdropping may be authorized for use by DoD criminal investigative agencies when there are reasonable grounds to believe that: 1. a criminal offense concerning the national security in involved; or 2. a felony has been or is about to be committed; or 3. telephone calls involved obscenity, harassment, extortion, bribery, or threat of bodily harm have been made to subscriber-user on a military base. The conditions under which such wiretapping or eavesdropping is conducted are specified in DoD Directive 5200.24.

Question 5. Does the Department ever utilize non telephonic electronic surveillance devices of any kind? If so, of what type and for what purposes?

Answer. As previously noted in the answer to question 4 above, the Department of Defense uses non-telephonic electronic surveillance devices. These devices include miniature transmitters, microphones and receivers which may use either wire or radio as a means of transmission. They are employed in criminal investigations primarily involving allegations of the sale of narcotics and dangerous drugs after responsible supervisory officials have determined that non-electronic investigative techniques would not provide the evidence needed or protect the military personnel involved. Their use is subject to the policies prescribed by the Attorney General.

Question 6. Does the Department possess tlephonic recording devices? If so, how many, and is a beeper or other warning device required to warn parties to the call of the recording?

Answer. Yes. Of of June 30, 1973, DoD possessed 755 telephone recording devices. DoD Directive 4640.1, "Telephone Monitoring," requires that any recording device used for office telephone monitoring must be equipped with a beeper or other warning devices. The use of the warning tone is in addition to the requirement for prior consent by all parties participating. Warning devices are not used in connection with command center communications recording, communications security monitoring, communications management monitoring or telephone interceptions conducted during criminal investigations.

Sincerely,

D. O. Cooke,
Deputy Assistant Secretary of Defense.

Attachments.

DEPARTMENT OF DEFENSE,
August 17, 1967.

DEPARTMENT OF DEFENSE DIRECTIVE

Subject: Telephone Interception and Eavesdropping

References: (a) Section 605 of the Communications Act of 1934, as amended (47 U.S.C. 605)
(b) Presidential Memorandum for the Heads of Executive Departments and Agencies, June 30, 1965
(c) Memorandum to the Heads of Executive Department and Agencies from the Attorney General, June 16, 1967
(d) Deputy Secretary of Defense Multiple-addressee Memorandum, "Reporting Interception Activities," August 10, 1966 (C) (hereby cancelled)

I. PURPOSE AND SCOPE

This Directive implements references (a), (b) and (c), and sets forth the policies and restrictions governing telephone interception and eavesdropping by DoD personnel engaged in the conduct of investigations for law enforcement purposes in the United States. It also establishes certain worldwide reporting requirements regarding storage, inventory, and use of interception and eavesdropping devices by DoD Components in the conduct of such activities.

II. CANCELLATION

Reference (d) is hereby superseded and cancelled.

III. APPLICABILITY

This Directive is applicable to all DoD Components. It does not apply to activities which are related directly to the protection of the national security.

IV. DEFINITIONS

For the purpose of this Directive, the following definitions apply:

A. *Wiretapping*—the act of listening to or recording of any telephonic conversation by the use of any electronic, mechanical, or other device without the advance consent of all of the parties to the conversation; sometimes referred to herein as interception.

B. *Eavesdropping*—the act of listening to or recording of any conversation other than telephonic by the use of any electronic, mechanical, or other device without the advance consent of all of the parties to the conversation.

C. *Heads of DoD Components*—the Secretaries of the Military Departments (or if they so designate, the Under Secretary, Assistant Secretary, the principal staff officer responsible for the investigative activity concerned, or the head of the investigative agency concerned), the Directors of the Defense Agencies, the Chairman of the Joint Chiefs of Staff, and the Assistant Secretary of Defense and other activities assigned for administrative support.

V. WIRETAPPING

A. To insure the privacy of telephone conversations to the maximum practical extent, the interception of telephone conversations is prohibited unless there are reasonable grounds to believe that:

1. A criminal offense concerning the national security is involved; or,

2. A felony has been or is about to be committed; or,

3. Telephone calls involving obscenity, harassment, extortion, bribery, or threat of bodily harm have been made to a subscriber-user on a military base under the jurisdiction of the Department of Defense.

B. National Security Investigations—The following requirements must be met:

1. One of the parties has freely and voluntarily consented in advance to the interception. If none of the parties has consented in advance, the interception must be approved by the Attorney General in advance, see paragraph V.F.3., below; and,

2. The interception has been approved in advance by the Secretary of the Military Department concerned (or his specific designee), or the Assistant Secretary of Defense (Administration) for all other DoD Components.

C. Felony Investigations—The following requirements must be met:

1. One of the parties has freely and voluntarily consented in advance to the interception; and,

2. The interception has been approved in advance by the Secretary of the Military Department concerned (or his specific designee), or the Assistant Secretary of Defense (Administration) for all other DoD Components.

D. Investigations Involving On-Base Telephones—The following requirements must be met:

1. The subscriber-user of the telephone has requested the investigation of telephone calls involving obsecurity, harassment, extortion, bribery, or threat of bodily harm and, in writing, freely and voluntarily consents in advance to the wiretap; and,

2. The telephone and wiretap are located on an installation under the jurisdiction of the Department of Defense; and,

3. The head of the investigative unit has approved the interception in advance in accordance with the rules prescribed by the Head of the DoD Component concerned.

E. The prohibitions and restrictions of this Section V. apply whether or not the information which may be acquired through interception is intended to be used in any way or to be subsequently divulged outside the Department of Defense. Any question as to whether the use of a particular device can be said to involve a prohibited interception of a telephone conversation shall be submitted to the General Counsel of the Department of a Defense for consideration.

F. A request for approval under subsections V.B. and C., above, shall include the information outlined in Enclosure 1.

1. Approval will not be granted for more than 30 days, and the wiretap will be terminated as soon as the desired information is obtained.

2. Renewal requests for specified periods of not more than than 30 days may be submitted to the appropriate approval authority fo reconsideration.

3. If the approval of the Attorney General is required, the request shall be sent to the Assistant Secretary of Defense (Administration) who, if he considers it justified, will forward it, and subsequent renewals thereof, to the Attorney General.

VI. EAVESDROPPING

A. To protect the rights of privacy, eavesdropping is prohibited if the listening to or recording of a conversation involves a violation of the Constitution or a statute. This prohibition includes eavesdropping in any form which is accomplished by means of physical trespass or entry. It also may include eavesdropping practices which intrude upon the conversations between persons whose relationship is traditionally considered privileged (such as lawyer-client and doctor-patient). Further, even though it may be accomplished without physical trespass or entry, it may also be unlawful if it invades the sanctity of a man's home, private office, hotel room, automobile, or other physical areas deserving protection of the right to privacy.

B. In order to limit eavesdropping not otherwise prohibited by subsection VI.A., above, eavesdropping is authorized without the consent of all of the parties only under the following conditions:

1. There are reasonable grounds to believe that a criminal offense concerning the national security is involved, or that a felony has been or is about to be committed; and,

2. Advance written approval has been obtained from the Attorney General, see paragraph VI.B.3., below. A request for approval under this paragraph must include the information outlined in Enclosure 1. Approval will not be granted for more than 30 days, and the eavesdrop will be terminated as soon as the desired information is obtained; and,

3. The request shall be sent to the Assistant Secretary of Defense (Administration) who, if he considers it justified, will forward it, and subsequent renewals thereof for not more than 30 days, to the Attorney General.

C. If, in the judgment of the Head of the DoD Component concerned, or his specific designee, the emergency needs of an investigation preclude obtaining the advance approval of the Attorney General as required by paragraph VI.B.2., above, he may, without that approval, authorize the eavesdropping required by the investigation. He shall, within 24 hours after authorizing the eavesdropping, provide the Attorney General, with a copy to the Assistant Secretary of Defense (Administration), with the information outlined in Enclosure 1. He shall include an explanation of the circumstances upon which he based his judgment that the emergency needs of the investigation precluded the obtaining of the advance approval of the Attorney General.

VII. PROCEDURES AND REPORTS

A. The Head of each DoD Component concerned shall require, under the administrative controls provided by this Directive, the following.

1. That when wiretapping or eavesdropping is authorized, the investigative agent shall: a. If technically feasible, permanently record the conversations concerned on tape or other recording medium; b. preserve the recording, together with any logs, transcripts, summaries, or memoranda that are made concerning the conversations; and, c. report in writing to the Head of the DoD Component describing the uses made of each device for wiretapping or eavesdropping.

2. As to information obtained by wiretapping or eavesdropping, that: a. Information is stored in an appropriate investigative file at a central location; b. information so stored is always identified, when used for any purpose, as information obtained by wiretapping or eavesdropping; c. access to information so stored is strictly controlled and recorded; and, d. information so stored shall not be disclosed outside the Department of Defense unless the Head of the DoD Component concerned determines that disclosure is essential to governmental operations.

3. As to records and devices used for wiretapping and eavesdropping, that: a. Devices are obtained only to the extent necessary for use in conformance with this Directive; b. units be designated to maintain and control devices; c. centralized records be maintained of the inventory and use of devices. (A record must include the date a device was assigned to an agent, the date he returned it, and his report under subparagraph VII.A.1.c., above, on its use); d. the need for devices be re-evaluated once a year; and, e. all records are maintained for a period of six years.

B. The Head of each DoD Component shall report to the Assistant Secretary of Defense (Administration) as follows:

1. Before the tenth day of each month stating whether there was any wiretapping or eavesdropping during the preceding month by personnel of the DoD Component concerned (a) in the United States or (b) elsewhere, if any party to the conversation was a citizen of the United States. The report must include all information in Enclosure 2.

2. Before July 10, annually, giving a complete inventory of all devices in the DoD Component concerned that are *primarily* designed for wiretapping or eavesdropping. The report shall include a statement that the inventory is being maintained at the lowest level that is consistent with operational requirements.

C. The Assistant Secretary of Defense (Administration) shall report by July 31, annually, to the Attorney General on all uses of devices for wiretapping and eavesdropping in the Department of Defense during the previous fiscal year, to include, in each case, the information in Enclosure 2. The report shall contain the Department of Defense inventory of devices.

VIII. REPORT CONTROL SYMBOLS

The reports required by paragraphs VII.B.1. and VII.B.2. have been assigned Report Control Symbol DD-A(M)795 and Report Control Symbol DD-A(A)796, respectively.

IX. EFFECTIVE DATE IMPLEMENTATION

This Directive is effective immediately. Two (2) copies of the implementing instruction shall be forwarded to the Assistant Secretary of Defense (Administration) within sixty (60) days. When implementation is contained in more than one issuance, one complete set shall be appropriately marked to indicate the implemented sections of this Directive. Two (2) copies of superseding, supplementing, or amending issuance will be forwarded to the Assistant Secretary of Defense (Administration) no later than fifteen (15) days after publication.

ROBERT S. MCNAMARA,
Secretary of Defense.

Enclosures.

INFORMATION TO BE INCLUDED IN A REQUEST FOR APPROVAL OF PROPOSED WIRETAPPING OR EAVESDROPPING

1. Indicate whether the request is for a wiretap or an eavesdrop.
2. The purpose. To the extent possible, describe the conversation expected to be intercepted.
3. Identity of all persons under investigation, or affected.
4. Statement if any party has consented, and if so, his identity.
5. With respect to the particular operation: a. Identity of the operating unit; b. types of equipment to be used, if any, to include method of transmission and recording device; c. manner or method of installation; d. physical location, to include the address, telephone number, room number, whether inside or outside a building, public or private property, and the means of access; and e. the expected period of time for the operation. (The period should be as short as possible compatible with operational necessity).

INFORMATION TO BE INCLUDED IN WIRETAPPING OR EAVESDROPPING REPORTS

1. Indicate whether the report is on a wiretap or an eavesdrop.
2. Identity of the persons against whom directed
3. Location.
4. Identity of the performing organizational unit.
5. Type of equipment used and manner and method of installation.
6. Approval authority.
7. Duration.
8. Purpose served.
9. Evaluation of results of operations that were completed during the reporting period.

Mr. LEHMAN. Is that the most recent DOD written policy, on eavesdropping?

Mr. COOKE. Well, let me make this observation. That directive is in the process of revision. It is the most recent official directive. But, of course, it has also been supplemented and the procedures are consistent with the Attorney General's 1972 memorandum, which we discussed earlier.

Mr. LEHMAN. Of course, that 1972 memorandum covers consensual wiretaps.

Mr. COOKE. As I indicated, we are not involved in the business of nonconsensual wiretaps.

Mr. LEHMAN. Nevertheless, you could conduct nonconsensual eavesdropping under a court warrant, could you not? And does not the 1968 law, which postdates your regulation, provide certain——

Mr. COOKE. Yes, we could. As a matter of fact, the regulation, the directive so provides. But, in the case that we wanted to conduct a nonconsensual within the meaning of title III, we would have to go

to the Attorney General and he presumably would have to, following his procedures, would have to get court authorization. But, the point I want to make that since the passage of the law, we have not had the occasion to do that.

Mr. LEHMAN. If one of our military investigative agencies wanted right now to conduct such a surveillance, how would they know that a court order was required, if the regulation predates the present law?

Mr. COOKE. Well, the regulation, as it now stands, shows that request has to come up to the head of the DOD component or his designee, with certain specified information. That, in turn, comes to my office and I would send it under the terms of the regulations, as it now exists, to the Attorney General, and they would not move without the consent. So, once it is sent up to me and it comes up to me, not only for the consensual eavesdrops we are talking about, in accordance with the Attorney General's memorandum, but in the event, which I emphasize has not occurred, of a nonconsensual, it would be treated the same way and it would go over to the Attorney General. And then we would need his approval, and I would presume that the Attorney General would then seek the court authorization. The directives does not give either to one of our criminal investigative agencies, or, for that matter, to the Secretary of Defense the right to apply directly to the court.

Mr. LEHMAN. Do you anticipate that very shortly you will be coming out with a new directive which will recognize title III of the 1968 law?

Mr. COOKE. Yes. As I indicated, I think our directive plus some modifications incorporated in the Attorney General's memorandum, are fully consistent with title III. But, like any other piece of official paper they should be updated and clarified with experience.

Mr. LEHMAN. And you have plans to?

Mr. COOKE. We have a draft revision well underway. I am not going to say 2 weeks from now, or 2 months from now, but they are well underway.

Mr. LEHMAN. I have one other question, and I am not sure that you covered it previously in your testimony. That is, what is the legal authority which the Department relies on for surveillance for American citizens outside of the United States? What statutory or judicial authority would you have for that?

Mr. COOKE. First of all, I share the opinion expressed by the Assistant Attorney General, Petersen, that the dividing line, obvious, is not or should not be citizen, noncitizen. The provisions of title III expressly exclude in their geographical application any activity conducted outside of the United States, its territories and possessions. I think the test is the function of the American citizens, some of them in uniform, by the way, and most of them in uniform in Europe and elsewhere. I am not aware of any statutory, judicial restrictions, talking of any limitation on surveillance overseas.

Mr. LEHMAN. Is it your impression then that the fourth amendment requiring, of course, court approval of wiretapping does not apply to American citizens living overseas?

Mr. COOKE. No. I certainly would not want to go that far. And I would think that any activity we undertake overseas is certainly consensual within the meaning of section 2511 of the U.S. Code. And, apparently, to the extent to which the Public Law 9351 treated the problem, it made that distinction by limiting its application to the United States, its territories and possessions.

Mr. LEHMAN. Was the wiretap involved in the *Berlin Democratic Club* case, was that a consensual wiretap?

Mr. COOKE. I am really not that familiar with the case. As I said, these are allegations in pending litigation, and I certainly am not familiar with the facts of the case.

Mr. LEHMAN. So, it is your position that among those overseas wiretaps which you gave us some statistics on just a few minutes ago, none were anything other than consensual wiretaps?

Mr. COOKE. As they are defined by the law, yes. And let me also assure you, and I will repeat this again, that any of our activities overseas are very carefully circumscribed by the Status of Forces Agreement, by the laws of the host nation and the like.

Mr. LEHMAN. So you do not conduct eavesdropping without the consent of at least one party to the conversation overseas on American citizens? Can you make that flat statement?

Mr. COOKE. No, I certainly cannot make that flat statement, particularly since, as I pointed out, and you had an extended discussion with the Assistant Attorney General on the problems of intelligence, positive intelligence connections.

Mr. DRINAN. Thank you, Counsel.

I have one additional question.

On page 10 of your testimony, you cite DOD Directive 5200.24, and I find it troublesome because the directive is, in my judgment, rather vague, in that information so stored shall not be disclosed outside the Department of Defense unless the head of the DOD component concerned determines that disclosure is essential to governmental operations. And I think you would have to admit that that is a pretty vague and ambiguous norm, especially Government operations. I am wondering if there is any record that the head of each DOD component must make, when he reveals his information outside of DOD, and what would "esssential to Government operations" mean in reality?

Mr. COOKE. I am not aware of a record. I can check that for you, Mr. Drinan. But, I would suspect it might be, particularly in many of our drug abuse cases where we are working very closely with the Bureau, or perhaps local authorities, where civilian pushers are involved, as well as military wholesalers selling to our people on base. And I think that clearly that would come under the provisions of essential governmental purposes.

Mr. DRINAN. Well, the regulation does not say that at all.

Mr. COOKE. I realize that the regulation in that regard is somewhat broadly worded.

Mr. DRINAN. How many people would there be in the category of heads of the DOD components?

Mr. COOKE. Essentially it is the Secretary of the Army, Navy, Air Force, that have the criminal investigative agencies under their juris-

dictions, and it would be they or their designee, a specific designee and not a blanket designation.

Mr. DRINAN. If I may ask you or your aides, is there any record of complaints by people who feel that their privacy has been invaded by this frankly very sloppy, regulation?

Mr. COOKE. We have had no record of complaints on the basis of this directive as such. As you are aware, we are in some pending litigation. The most current of that litigation now is the *Berlin Democratic Club* against *Schlesinger et al.*

Mr. DRINAN. Mr. Smith?

Mr. SMITH. No questions.

Mr. DRINAN. One final question:

Did you have any suggestion for the committee as to what areas of privacy we could protect?

Mr. COOKE. I have no specific suggestion at this time.

Mr. DRINAN. All right. Thank you very much, sir.

[The statement of Secretary Cooke follows:]

STATEMENT OF DAVID O. COOKE, DEPUTY ASSISTANT SECRETARY OF DEFENSE

Mr. Chairman and Members of the Committee, I am here in response to your invitation to the Secretary of Defense to furnish information in connection with your inquiry into changes to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, and to provide information relating to the policies and procedures by which wiretapping and electronic surveillance are authorized and controlled within the Department of Defense.

For management purposes, the Department has placed wiretapping and electronic surveillance activities into two separate categories.

Departmental policies and procedures which limit the use of telephone monitoring and control the use of information obtained by third parties, are set forth in Department of Defense Directive 4640.1, "Telephone Monitoring." DoD policies which restrict the use of wiretapping and eavesdropping during the conduct of investigations for law enforcement purposes are published in DoD Directive 5200.24, "Telephone Interception and Eavesdropping." Both of these directives apply to the United States, the Commonwealth of Puerto Rico and U. S. territories. They do not apply elsewhere overseas, nor are they applicable to our foreign intelligence collection activities. Copies of the two Directives were provided to your Committee last week.

First, I would like to discuss telephone monitoring which is administrative rather than investigative in purpose. There are four classes of telephone monitoring. They are:

Office telephone.—Listening to or recording office telephone communications by use of mechanical or electronic devices or recording by written means, for the purpose of obtaining an exact reproduction or a summary of the substance of the telephone conversation and with the consent of all parties.

Command center communications.—Listening to or recording telephone communications in DoD command centers for the purpose of obtaining a record of conversations, or parts thereof, for command and control purposes.

Communications security.—Listening to or recording of the transmission of official defense information over DoD-owned or leased telephone communications, by any means, for the purpose of determining whether such information is being properly protected in the interest of national security. Notice of this action is given to users that these systems are subject to communications security monitoring at all times.

Communications management.—Listening to or recording telephone communications on DoD-dedicated systems or the common-user systems of the Defense Communications System, by any means, not for the contents but for the purpose of determining whether the systems are functioning properly for official purposes. Almost every phone company has a counterpart activity.

The first class of telephone monitoring is one in which you are all familiar, called office monitoring. With the use of either a recorder equipped with

"beeper" or with a stenographer, it requires the advance consent of all parties to the conversation. Office telephone monitoring, in such cases, is a valuable management tool to reflect the exact nature of agreements and understandings achieved by telephone. One of the parties to the conversation may be outside the DoD but again let me emphasize that all parties concerned must consent to office telephone monitoring.

The other three classes of telephone monitoring are largely internal. That is, they are directed to the manner in which DoD military and civilian personnel use telephones which are part of DoD communications systems.

Telephone monitoring in command centers, for communications security and for communications management purposes, does not require express consent in each case. The purpose of command center monitoring is to obtain accurate records for command and control purposes of official calls to a command center. Examples of the Command Centers are the National Military Command Center, its Alterate, the Airborne Command Post, the North American Air Defense Command Post, the Military Services Operations Centers in Washington, the Military and Security Police Operations Centers, Fire and Rescue Control Centers and Air Traffic Control Centers.

DoD monitoring for these Centers closely compares with the recordings made by the Federal Aviation Agency in its many air traffic control centers. Similarly, most police, fire, and rescue control centers in our large cities and counties monitor incident reports and requests for assistance to insure accuracy and for record purposes. Furthermore, command centers are able to record messages to be rebroadcast to subordinate and lateral units.

DoD Directive 4640.1 requires for each center specific regulations be published prior to the initial operation of the recording equipment The existence of such monitoring, however, is required by DoD Directive 4640.1 to be so widely and expressly publicized throughout DoD and its components as to amount to constructive consent.

Our authority for this class of monitoring equipment and its use stems from communications common carrier tariffs which have been approved by the Federal Communications Commission. This class of monitoring is provided for in DoD Directive 4640.1, which I mentioned earlier.

Communications security monitoring (COMSEC monitoring) is the third class of administrative telephone monitoring wihch is used albeit rarely on Department of Defense telephone circuits. The purpose of COMSEC monitoring is to provide a basis for analysis to ensure that classified information is not discussed on unsecure telephones.

This monitoring may only be conducted when authorized by the Commander or DoD official in charge of an installation or activity or his superior. Let me stress that security organizations organized and equipped to perform communications security monitoring are not authorized to monitor communications systems on their own initiative. Communications security monitoring is employed infrequently. Less than 1% of our telephones are monitored for security in any given year.

The lines selected for security monitoring consist mainly of command posts, major operational headquarters, war rooms, and field exercises both in the United States and overseas.

Let me emphasize that the purpose of COMSEC monitoring are to advise commanders on actual or possible security compromises and improve the security protection of telephone communications.

DoD 4640.1 expressly states that the information obtained as a result of telephone communications security monitoring shall not be authorized for law enforcement purposes unless the General Counsel authorizes an exception in a specific case.

The last class of administrative telephone monitoring is Communications Management Monitoring, often called service observation. Service observation is conducted largely by computer analysis and pay count methods rather than by actual listening to telephone conversations in progress.

It is a tool used to determine if telephone systems are functioning properly, not with the contents of conversations, but with such things as the precedence and number of calls, their duration, response to signals, number of busy signals for a given time period, total load on a system in numbers and duration of calls, etc.

The purpose of administrative telephone monitoring previously described is distinctly different from the purpose of wiretapping or eavesdropping. Telephone monitoring is to accurately preserve records of conversations as in command centers or to analyze a total system for adherence to protection of classified information as in COMSEC monitoring.

Wiretapping and eavesdropping are used for the purpose of criminal investigations.

Let me now turn to the Department's policies and procedures for telephone interception and eavesdropping techniques used in investigating criminal cases. DoD defines these terms exactly as they are defined in Title III of Public Law 90-351:

Telephone Interception (Wiretapping).—The use of electronic, mechanical, or other devices to intercept a wire communication for the purpose of obtaining information as part of a criminal investigation.

Eavesdropping (Electronic Surveillance).—The use of electronic, mechanical, or other devices to intercept an oral communication for the purpose of obtaining information as part of a criminal investigation.

Directive 5200.24 authorizes under controlled circumstances the use of telephone interception (or wiretapping) and non-telephonic electronic surveillance (eavesdropping) by DoD criminal and investigative agencies when there are reasonable grounds to believe that: 1. a criminal offense concerning the national security is involved; or 2. a felony has been or is about to be committed; or 3. telephone calls involved obscenity, harassment, extortion, bribery, or threat of bodily harm have been made to a subscriber-user on a military base.

Wiretap and eavesdrop operations conducted by DoD are in full compliance with the policies and requirements established by the Attorney General and issued pursuant to 18 U.S. Code, Chapter 119.

Let me stress most strongly that the DoD is *not* in the business of conducing electronic surveillance of civilians not affiliated with the Department. DoD Directive 5200.27 expressly *forbids* such practices except in narrowly defined circumstances. In other words, the wiretaps or eavesdrops DoD conducts are employed only in cases involving military or, in extremely rare cases, DoD civilian personnel *provided the FBI has yielded jurisdiction.*

The procedures I am about to describe are those instituted by the Attorney General for consensual wire taps and eavesdrops. That is, at least one party has consented. All non-consensual cases, should any arise, must be referred to the Attorney General. *None* have arisen in DoD since the passage of PL 90-351 in 1968.

Under the Attorney General's procedures and the provisions of DoD 5200.24, consensual wiretaps may be authoribed by heads of DoD Components or their designees for the investigation of criminal cases and harassing telephone calls. DoD Components have issued regulations setting forth procedures and controls for these authorizations.

The Attorney General has adopted stricter rules in the case of eavesdrops. For consensual eavesdropping of non-telephonic conversations, prior approval normally must be obtained from the Department of Justice. Again, DoD Directive 5200.24 provides first that the head of the DoD Component concerned, or his designee, must approve the proposed eavesdrop. Then it must be approved by the DASD/A before it is sent to the Attorney General requesting his approval. Attorney General regulations provide for emergency monitoring in advance of his approval to prevent the imminent loss of essential evidence. In such cases, a full report of justification must be provided to him.

Each request for approval of proposed wiretapping or eavesdropping must contain a detailed statement as to the crimes and persons involved and a statement that the consent of one party has been obtained with his identity. All approvals are limited to 30 days, as are any renewals.

DoD Directive 5200.24 provides careful safeguards both as to the integrity of equipment and any information obtained by their use.

The wiretapping and eavesdropping devices are carefully accounted for and stored under secure conditions by the investigative agencies of our Military Departments. Both categories of electronic devices are only authorized for use in approved cases under the supervision of experienced agents who have been instructed in the legal and private rights aspects of their use.

With respect to the information that might be received by wiretapping or eavesdropping activities, DoD 5200.24 requires that it be stored in appropriate investigative files at a central location; that the information so stored is always identified, when used for any purpose, as information which was obtained by wiretapping or eavesdropping; that access to information so stored is strictly controlled and recorded; and that this information shall not be disclosed outside of the Department of Defense unless the head of the DoD Component concerned determines that disclosure is essential to governmental operations.

Finally. the Directive requires quarterly reports to the Secretary of Defense concerning the employment of wiretaps and eavesdrops, incluiding those conducted in areas of the world where the substantive provisions of the Directive do not apply. We also have an annual summary and electronic equipment report to make to the Attorney General.

In recent years, wiretapping has shown an increase in cases involving drugs and telephonic bomb threats or other harassing calls. Eavesdropping activities have shown a marked increase over the last several years attributable almost completely to the narcotics and drug problem.

Consensual intercepts, particularly eavesdrops, have contributed significantly to our success in drug cases. However, because of the type and short duration of the calls, we have been only moderately successful in identifying the callers in bomb threats and similar cases. Both wiretapping and eavesdropping are essential elements in the DoD law enforcement program.

Department of Defense programs and activities under DoD 5200.24 which have been discussed would be affected adversely by pending legislation relating to wiretapping and electronic surveillance. In particular H.R. 9698 would prohibit the interception of certain communications unless all parties to the intercepted communication consent. The effect of H.R. 9698 would be to eliminate the use of wiretaps or eavesdrops in any criminal case. Obviously, none of the narcotic and drug cases which the Military Services have investigated successfully on the basis of consensual intercepts undertaken in accord with the present law would have been possible if the prior consent of *each* of the parties had been a necessity.

The bill, in my judgment, would not impact on our administrative telephone monitoring procedures which are now based on actual or implied consent of all parties.

Mr. Chairman, I have appreciated the opportunity you have afforded the DoD to describe its policies and practices in the area of electronic surveillance. We realize that this is an area of balancing the rights of the individual on one hand and the legitimate needs of an organized society on the other. We believe our directives are not only in full compliance with the law and the Attorney General's regulation but also have achieved that balance.

Mr. DRINAN. Mr. William Caming is our next witness, appearing on behalf of the American Telephone & Telegraph Co. Mr. Caming is the attorney chiefly responsible for all security matters within the Bell System, a system which consists of 24 operating companies and handles over 85 percent of all telephone calls in the United States.

Welcome, Mr. Caming, and proceed with your testimony if you will.

TESTIMONY OF HON. WILLIAM CAMING, ESQ., ATTORNEY, AMERICAN TELEPHONE & TELEGRAPH CO.

Mr. CAMING. Thank you, and good morning, or good afternoon, at this moment.

I will attempt to summarize the testimony contained in our statement.

Since 1965, I have had primary responsibility from a legal standpoint for oversight over matters pertaining to industrial security and privacy, as they affect the Bell System.

I wish to thank the subcommittee for the opportunity to present the views of the Bell System on privacy of communications and delineate our experiences with electronic surveillance, principally in the area of wiretapping.

At the outset, I wish to stress the singular importance the Bell System has always placed upon preparing the privacy of telephone communications. Such privacy is a very basic concept in our business. We believe that our customers have an inherent right to feel that they can use the telephone with the same degree of privacy they enjoy when talking face to face. Any undermining of this confidence would seriously impair the usefulness and value of telephone communications, in our opinion.

Over the years, the Bell System has repeatedly urged that full protection be accorded to its customers' privacy, and we have constantly endorsed legislation both at the Federal and State level, that would make wiretapping as such illegal. In 1966 and again in 1967, we testified to this effect before the Senate Subcommittee on Administrative Practice and Procedure during its consideration of the Federal omnibus crime control and safe streets bill. This is still, of course, our position.

We believe that the Federal Omnibus Crime Control Act has contributed significantly to protecting privacy by, among others, clarifying existing law and proscribing under pain of heavy criminal penalty any unauthorized interception or disclosure or use of a wire communication. I might parenthetically state that thertofore interception and disclosure was a requirement under section 605.

During our congressional testimony, we said too at that time that we recognized that national security and organized racketeering are matters of grave concern to the Government and to all of us as good citizens. The extent to which privacy of communications should yield and where the line between privacy and police powers should be drawn in the public interest are in our opinion, matters of national public policy, to be determined by the Congress upon a proper balancing of the individual and societal considerations.

For more than three decades, it has been Bell System policy to refuse to accept in the yellow pages of its telephone directories advertisements by private detective agencies and others, stating or implying that the services being offered include the use of wiretapping. In December 1966, during congressional consideration of the Federal Omnibus Crime Control Act's Title III proscriptions against unauthorized interceptions, this longstanding policy was expanded to prohibit too the acceptance of eavesdropping copy. This standard, adopted by all Bell System Cos., was interpreted from the outset to make equally unacceptable so-called debuging advertising.

The removal of unacceptable copy is a never-ending task of large proportions, since many such advertisements are revised, and new outset to make equally unacceptable so-called debugging advertising. ones appear, in each issue of our 2,400 directories. We believe, however, that we have done a creditable job in this area, and we intend to continue such rigid policing as contributive to maximizing privacy of communications.

It may help place matters in perspective if we provide a brief insight into the magnitude of telephone calling that occurs in this country in a single year. During the calendar year 1973, for example, there were approximately 138 million telephones—including extensions—in use in the United States, from which some 188 billion calls were completed.

From the time our business began some 90 years ago, the American public has understood that the telephone service they were receiving was being personally furnished by switchboard operators, telephone installers, and central office repairmen who, in the performance of their duties of completing calls, installing phones, and maintaining equipment, must of necessity have access to customers' lines to carry out their normal job functions. We have always recognized this and have worked hard and, we believe, effectively to insure that unwarranted intrusions on customers' telephone conversations do not occur.

The advance of telephone technology has in itself produced an increasing measure of protection for telephone users. Today, the vast majority of calls are dialed by the customer, without the presence of an operator on the connection. This has greatly minimized the opportunities for intrusions on privacy. There are many other technical advances of similar import touched upon in our testimony.

Beyond this, all Bell System Cos. conduct a vigorous program to insure every reasonable precaution is taken to preserve privacy of communications through physical protection of telephone plant and thorough instruction of employees.

Our employees are selected, trained, and supervised with care. They are regularly reminded that, as a basic condition of employment, they must strictly adhere to company rules and applicable laws against unauthorized interception or disclosure of customers' conversations.

In regard to our operating plant, all of our premises housing central offices, equipment and wiring and the plant records of our facilities, including those serving each customer, are at all times kept locked or supervised by responsible management personnel, to deny unauthorized persons access thereto or specific knowledge thereof. We have some 90,000 people whose daily work assignments are in the outside plant. They are constantly alert for unauthorized connections or indications that telephone terminals or equipment have been tampered with.

With these measures and many others, we maintain security at a high level.

Our concern for the privacy of our customers is reflected too in the care with which we investigate any suspicious circumstances and all customer complaints that their lines are being wiretapped. Our companies follow generally similar operating procedures when an employee discovers a wiretap or eavesdropping device on a telephone line. Each of these cases is carefully checked. In those few instances where there is evidence of wiretapping, the employee discovering it is required to inform his supervisor immediately, and a thorough investigation is undertaken in every such case by competent security and plant forces.

In a small number of cases, a customer suspects a wiretap and asks for our assistance. Usually, these requests arise because the customer hears what are to him suspicious noises on his line. Hearing fragments of another conversation due to a defective cable, or tapping noises due to loose connections, or other plant troubles are on occasion understandably mistaken for wiretapping. Each company has established procedures for handling such requests. Generally, the first step is to have our craftsmen test the customer's line from the central office. In most instances, these tests will disclose a plant trouble condition. In each such case, the trouble is promptly corrected and the customer informed there was no wiretap.

In cases where no trouble is detected through testing the customer's line, a thorough physical inspection for evidence of a wiretap is made by trained personnel at the customer's premises and at all other locations where his circuitry might be exposed to a wiretap. If no evidence of a wiretap is found, the customer is so informed. Where evidence of a wiretap is found, the practice generally is to report to law enforcement authorities any device found in the course of the company inspection, for the purposes of determining whether the device was lawful and of affording law enforcement an opportunity to investigate if the tap was unlawful. The existence of the device is also reported to the customer requesting the check, generally irrespective of whether it was lawful or unlawful. The customer is told that "a device" has been found on his line, without our characterizing it as lawful or unlawful; should the customer have any questions, he is referred without further comment to the appropriate law enforcement authority.

New Jersey Bell, however, as a matter of policy, informs a customer requesting a wiretap check that only the presence of an unauthorized device will be disclosed. Minnesota by statute similarly limits disclosure to unlawful devices. Should the customer inquire about the presence of a lawful device, he will usually be assured that applicable Federal and State laws require any judge authorizing or approving a court-ordered interception to notify the affected customer within 90 days after interception ceases—or at a later date, if disclosure is postponed upon a good cause showing by law enforcement. Section 2518(8) of title III provides that provision under law.

All Bell System Cos. report the existence of an unlawful device to the customer requesting the check, as well as to law enforcement, and the latter is provided an opportunity to invesetigate for a reasonable period—generally 24–48 hours—prior to removal of the wiretap.

We might point out that unless the wiretap effort is amateurish, a person whose line is being tapped will not hear anything unusual, because of the sophisticated devices employed. As we previously said, most of the complaints originate because the customer hears an odd noise, static, clicking, or other unusual manifestation. As far as our experience discloses, these usually turn out to be difficulties in transmission or other plant irregularities. From 1967 onward, for example, the total number of wiretap and eavesdrop devices of all types—including both lawful and unlawful—found by telephone

employees on Bell System lines has averaged less than 21 per month—an average of less than one a month for each of the twenty-four operating companies of the Bell System. In our opinion, the criminal sanctions imposed by title III—for the authorized interception or disclosure or use of wire or oral communications, or the manufacture, distribution, possession, or advertising of intercepting devices—coupled with vigorous law enforcement and attendant publicity, appear to have contributed significantly to safeguarding telephone privacy.

In the area of court-ordered wiretapping, it is the policy of the Bell System to cooperate with duly authorized law enforcement authorities in their execution of lawful interceptions but only to the extent of providing limited assistance as necessary for law enforcement to effectuate the particular wiretap. We wish to stress that the Bell System does not do the wiretapping. The assistance furnished generally takes the form of providing line access information, upon the presentation of a court order valid on its face, as to the cable and pair designations and multiple appearances of the terminals of the specific telephone lines judicially approved for interception in the court order. In the instance of law enforcement authorities of the Federal government and of those States enacting specific enabling legislation, and I believe there are seven in number and the District of Columbia, the court order may direct the telephone company to provide limited assistance in the form of the information, facilities and technical assistance necessary to accomplish the wiretap unobtrusively, and with a minimum disruption of service.

Upon the receipt of such a directive in a court order valid on its face, our cooperation will usually take the form of furnishing a private line channel from terminal to terminal—i.e., a channel from a terminal which also services the telephone line under investigation to a terminal servicing the listening post location designated by law enforcement. Additionally, the above described line access information will be furnished for the specific telephone lines judicially approved for interception.

On occasion, assistance in the form of private line channels is furnished to Federal authorities in national security cases. This assistance is only rendered upon specific written request of the Attorney General of the United States or of the Director of the Federal Bureau of Investigation—upon the specific written authorization of the Attorney General to make such request—to the local telephone company for such facilities, as a necessary investigative technique, and it is so stated, under the Presidential power to protect the national security against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. For reasons of security, we are not informed in such cases of the specific nature of the national security matter under investigation. And we strictly ensure that we don't need any such information, in order to maximize its security.

In cooperating in court-ordered and national security cases, we endeavor to provide the very minimum assistance necessary as re-

quired by law, to effectuate the particular wiretap. Under no circumstances, do we do the wiretapping itself; that is the exclusive province of the appropriate law enforcement officers. Nor do we furnish end equipment to be used in connection with a wiretap, such as tape recorders or pen registers. Nor do we design or build wiretap or eavesdrop devices for law enforcement authorities. Furthermore, our telephone companies do not train law enforcement personnel in the general methods of wiretapping and eavesdropping, nor do we provide telephone company employee identification cards, uniforms or tools, or telephone company trucks.

In conclusion, I wish to assure you based upon almost nine years experience in this area personally, that the Bell System continues to be wholly dedicated to the proposition that the public is entitled to telephone communications free from unlawful interception or divulgence. We are vitally interested in the protection of the privacy of communications and always welcome measures and techniques that will strengthen and preserve it.

I shall be pleased to endeavor to answer any questions that the Subcommittee may have.

Mr. KASTENMEIER. Thank you very much for what I consider an extremely helpful testimony, Mr. Caming. And I only apologize that at the outset of your testimony, I was called away and was not present. But, I have had an opportunity to read your statement and hear you deliver most of it.

There are some questions which arise, which seem to me procedural questions. Who makes the decision in the telephone company as to whether to cooperate with the person who represents himself as the representative of a Federal agency who is authorizd to conduct a tap? Is that decided at each local office?

Mr. CAMING. No. May I?

Mr. KASTENMEIER. Yes.

Mr. CAMING. Sort of walk through this or stumble through it with you and see if I can help.

First, in each Bell System Co. we have a security group headed by a security manager. All of the personnel involved are carefully trained, and they are long-term employees in almost all instances, and very qualified and, of course, as responsible and reliable people as we have.

We also have in each company, just so that you can get the full picture, a legal department which varies in size, but in each case has a security counsel who is fully cognizant of just about everything that goes on, and that specifically, more or less is under my wing.

We also have at A.T. & T. a corporate director for security, and the head security managers are coordinated through his efforts. And he is one of my primary clients, as you could well imagine.

Now we do require that any order that is presented to us—and the personnel have been trained in security as to the qualifications that an order must possess in order to be valid on its face—and that has been very carefully reviewed with him. And I might say that most orders are very similar in tenor, as far as validity.

Mr. KASTENMEIER. But, Mr. Caming, are you referring to court orders?

Mr. CAMING. The court orders. And let us assume it is a member of the Federal Bureau of Investigation or a member of the Drug Enforcement Administration that is using the Federal authority, as an example. They are required to submit the order to the security manager. They cannot submit it to anyone else in the company. And, generally, they are familiar and so are the State and local authorities as to whom the proper individuals are. The security manager, or one of his specially trained security supervisors, and they are all in management, will then review the order. Now, he has been generally familiar with orders, and if the order appears on its face to be identical with proper orders, so far as form, he will then be in a position to pass upon its validity. If he has any question whatever, he has the strictest mandate to take it up with the secretary counsel. And if any question arises they immediately call me.

Mr. KASTENMEIER. Let me ask you this: That is fairly clear. There seem to be three areas; one, let us say, the private, unauthorized, illegal wiretapping, which you do not support in any sense, and you have indicated in your statement how your companies would handle this. Second, you have the taps for which there is a legitimate order or a warrant which is submitted to the Security Manager. And, third, the class of warrantless wiretaps for which there is no order given to you or to your Security Manager locally. How is that third class handled? What I have in mind, of course, is the point raised earlier by the gentleman from Massachusetts, Mr. Drinan. If somebody comes in and says, look, we want to tap Dr. Halperin for 22 months; we do not have an order for it, but we will just tell you that it is for national security. Are you not going to ask any questions? What happens in that case?

Mr. CAMING. All right. Let me tell you what our current procedures are and if you wish we can go back and can give you the history. I have gone over that with Mr. Lehman previously. I can do it very briefly or I can give you our present practice and then give you such history as you gentlemen may desire.

Mr. KASTENMEIER. I would be interested——

Mr. CAMING. Let me giving the existing, and then we can go back if you so desire.

Mr. KASTENMEIER. Yes. I think your practice since the 1968 law, authorizing wiretapping pursuant to warrant would be of interest to the subcommittee. I think that the 1968 act probably changed many things for your company and for the Government agencies conducting surveillance. Accordingly, I would think that during the last 6 years you might have developed a uniform policy.

Mr. CAMING. All right. Let me give you this very briefly, and when I say brief I usually am as much as a lawyer may, and Mr. Drinan would probably know that lawyers are not often very brief.

From the inception of national security wiretaps in 1941, as we know now—and I am quoting past history where I was still struggling through my last year in law school—with the war on at that time, wiretapping without warrants was introduced and a certain limited amount of cooperation was required from the telephone Co. Over the years, until the passage of the Crime Control Act, this was

handled with great sensitivity by our Company, perhaps because it was launched during World War II, perhaps because we try to be conscientious citizens. The matter of handling wiretaps was done with considerable delicacy, and usually the liaison point was especially designated and the only cooperation was extended to the Federal Bureau of Investigation, I might add, and would be some individual of relatively reasonably high position within the company and only he and others who had a need to know would ever know that such requests were made. And over the years, there were not too many. And we had the understanding from the inception, which was renewed over the years, that in each case there was a particular authorization from the Attorney General of the United States and that such authorization was in writing and was in the hands of the FBI or the Department of Justice to be recallable if necessary. For example, in litigation or perhaps before a committee of Congress.

It was agreed from the inception, too, that because these matters were too delicate, and I think the first ones only related you might say to foreign intelligence from 1941 on, it was decided that no paper trail should be left, so that no written matter was presented to us affirming this authorization, the idea being if anyone got access to it, it would disclose vital secrets.

Now, we became concerned starting in 1965, 1966, with the changes that had been revealed. The hearings before the Subcommittee on Administrative Practice and Procedure, starting in about May 1965, under the chairmanship of Senator Edward Long of Missouri, the fact that the military, to some extent, were engaging in somewhat publicized worldwide monitoring of some of their military exercises, and the general rising concern about privacy, and perhaps some of the questions raised in the Long committee about how the Government was using some of its wiretapping efforts. So, it was decided that it would be in the best interest, both of the Government and ourselves, to reduce to writing this commitment. This was not an easy decision, nor was it unanimous within the system. We have large independent entities as our Bell Telephone companies and we do not always agree. I think you could appreciate that even in the Congress there is not always complete agreement.

Mr. KASTENMEIER. There was evidence that the New Jersey Bell System distinguished itself in terms of policy from some of the other systems?

Mr. CAMING. In connection with national security?

Mr. SMITH. Mr. Chairman, I think the statement was that the New Jersey Bell Co., as a matter of policy, advised a customer only about unlawful wiretapping.

Mr. CAMING. Yes. That is what I call an expression of free spirit. And I just think the approach used by New Jersey Bell is possibly just as good. They and we have been troubled by the question which is left unanswered by the congressional legislative history of title III. Can we disclose an authorized device? Clearly we cannot disclose that it is authorized because both the court order and the underlying application are expressly sealed by statute, and under 2518(8) it is a contempt of court to disclose that. The question is,

what about a device we find that we know from an order in our possession, or from other means, perhaps querying law enforcement, being told, gentlemen, it is lawful, can we disclose this. And we have had some real conflicts with law enforcement who have, on pain of criminal contempt, told us that by disclosing the presence of a device we are giving away the fact that it is a lawful device and in their terminology, unearthing or blowing the investigation, and it is a matter of grave concern.

We have taken a very limited position because we have leaned over, in our opinion, as far as the law permits, to cooperate to as limited an extent as we can, and we have said that Congress sealed the order and sealed the application and they have sealed the device, too, as far as disclosure. They did not. And we have said that in the absence of a statute of a State, or a court mandate in a particular place, we will disclose the presence of the device and that is why I put in quotes in my statement the term "a device." Whether it is lawful or unlawful, we say we have found a device and if you have any questions whatever, talk to law enforcement. Therefore, the customer can never know whether or not it is a lawful or unlawful device. We have found thus that there would be no giveaway.

Now, New Jersey Bell, and Minnesota by statute, preclude that. They expressly prohibit the disclosure of a lawful device. In New Jersey they merely say on a form that they present to the customer when they request a check, and he gives his name and authorization to check his line, and they have a paragraph pointing out that the order and the application are sealed, and then they go on to say, and, accordingly, we cannot disclose the order or application nor will we disclose the presence of any device other than an unauthorized device. And then, as I mentioned in the statement, the customer says, well, that is great, but what about an authorized device? And we say, you have the assurance that 90 days normally after termination of any wiretap or eavesdrop the issuing or denying Judge, if he denies approval in a specific case, is required to disclose this. And I think that is the case that was alluded to in the statement. They both reached the same result, they both did not disclose the presence of a device. Except for New Jersey and Minnesota, we uniformly follow the other approach.

Mr. KASTENMEIER. We were, of course, pursuing the question of warrantless taps, which is a somewhat different situation, with respect to the person being tapped. Nothing is disclosed in 90 days or at any other time.

Mr. CAMING. Well, we would have a problem there. As you could appreciate, our role is really to carry out the necessary functions that our being guardians of the system requires.

Mr. KASTENMEIER. I appreciate that your general policy has been in aid of law enforcement.

Mr. CAMING. Well, our general policy has been primarily and first, and I can catalog it right now, in aid of privacy of communications, and second in being responsive to law enforcement really to the degree necessary under title III or national security, and there I would not use the word begrudging, but it has been ex-

tremely limited. We have refused to do a number of things which law enforcement has said we are required to do. We, for example, have in a particular circuit recently found to be in criminal contempt for refusing to give certain assistance of a limited nature, because we have felt it was not within the framework of the law as far as a present title III situation. And we did not voluntarily feel that it was advisable, on balancing the public interest as well as we could.

Mr. KASTENMEIER. Then you do, in fact, make a judgment about requests of you for warrantless wiretapping?

Mr. CAMING. Well, yes. We do require and we perhaps are getting back to the point where we got off onto New Jersey. If I may, in a national security situation, as I said, due to the concern expressed, and with negotiations with Mr. Vinson and others of Mr. Katzenback's group, and on later occasion with Mr. Clark and Mr. Yeagley of his Department, we forged a written understanding that only if such a request was presented to us for limited assistance in the form of private line channels would we cooperate in a national security situation. I might emphasize this was merely reducing to writing the understanding we have always had that there was written authorization, and that the matter was to be conducted by the FBI.

Now, in that case, when we do receive such a letter denominating a request as one in the national security interest, we do not attempt to evaluate it. I was referring to other situations, such as a situation where national security will not be present. This will parenthetically or must be signed by the Director of the Federal Bureau or by the Attorney General and, generally, it has been signed by the Director of the Federal Bureau.

Now since the *Keith* case, of course, we recognize it, and I know Mr. Maroney testified before the Congress in, I think, June of 1972, shortly after the *Keith* case, assuring the Congress that the Department would comply fully with its terms. And I think that was the testimony in the hearing which recently came to my attention.

Now, we cannot evaluate, and we do not know the purpose of the investigation. Often we will only in the letter get a location or telephone number. That matter goes to the security manager. All of our requests are concentrated in security. He handles it with just as much restrictive character as can be possible. Very few people in our company have access to these. For example, if there is a question arising with respect to one, even in discusions with me, I have assured that anything is blocked out that might be the facts, feeling that I have no need to know that in order to resolve the question. Now, we do not know and we will report frankly to the Department of Justice any agent that gives us any indication of a purpose of the investigation, the theory being that if it is significant enough to be national security, the security should be maximized.

Mr. KASTENMEIER. Is it not a fact that you did not require a request in writing for warrantless taps in Washington until 1973?

Mr. CAMING. No, that is not the fact. But, Mr. Lehman has reference to a point which we were coming to. As I said, we were just, up to 1968, we adopted the letter and then I did branch off perhaps

too quickly to the fact that the letter was adopted virtually in the fall of 1968, from our standpoint. It took the Department of Justice and ourselves a long while to hammer out the exact words, and who would sign it and whether it would be confined to the Attorney General or the Attorney General and the Director, and we finally agreed just on those two persons.

Now, in May 1969, the letter was finally sort of formalized and introduced in a meeting we had with all Bell System general security managers, and security counsel, to explain first the new title III procedures from our standpoint as to how we would handle them, because you may recall under Mr. Johnson, title III was not used so far as a court order provision. So, it was only in early 1969 that we had the problem of getting court orders, and at that same time we introduced this so-called letter which I have alluded to.

Now, it took us—there was a lot of dissension about the letter as I indicated, within our own ranks as to whether we were not creating a paper trail that might well disclose to the wrong eyes the particular activity under investigation. And were we not perhaps going too far. Now, this is a question which was freely discussed and we recognized there were viewpoints. But, gradually, over another long period of time the letter was introduced and in August, I think the meeting of August 4, 1971, the last company, the Chesapeake and Potomac Co. in Washington, used the letter. So, since then we have had the letter uniformly throughout, and that has been our practice until then.

Now, before then, a case arose which, of course, we did not know about at the time, as to the ramifications that have been disclosed, and the case was involving the wiretapping under the aegis of national security of some 17 members, 13 or 14 of whom were Government officials, and 4 of them were members of the press. One of the members of the Government I think was Mr. Halperin. Now, there is litigation pending on that, but I feel free to discuss at least our role, which was a very limited one of just processing facilities.

As I understood it, we received the oral request with the statement which happily now has been corroborated in the pleadings and I say "happily' because you can understand our position at that time, that was, one, that was a specifically authorized national security investigation and, two, we were advised on the foreign intelligence activities aegis of national security investigation. Whether that was true or not, of course, we have no way of determining and we still do not, on any of these. And, third, as I understood it and some of this is from subsequently published documents, because we are not privy to every one of these, at least it is one of their taps was for duration of May 1969 to February of 1971, and it may even have been of Mr. Halperin, although I am not sure without consulting my records. Some were of shorter duration of these 17. At that time, we had not adopted the letter. As I say, it was just at that time that it was coming in, so there was that juxtaposition, and even if we had had the letter though, we would have done exactly the same thing, and we would do it today, since we do not know normally, we may possibly identify a subject, if one of the security managers was curious enough, you know, to check, but normally we only are

advised of the location at which these take place and all we do is provide the channel from terminal to terminal, where they are taken. It may or may not be clear but we just get the telephone number and the channel, and we do not know the purpose of the investigation other than that we are assured by the Director of the FBI and in writing, or by the Attorney General that it is a foreign intelligence investigation.

Mr. KASTENMEIER. Let me ask you this, Mr. Caming.

Would it not be possible and perhaps even the practice at the Justice Department or the Bureau, whether they obtain a warrant or not, not to notify the phone company? They may not need your company's cooperation on certain taps. They may have the technical capacity to install those taps or devices without your knowledge or consent.

Mr. CAMING. I think this is very true and is the fact in this sense, not that they do it improperly but, first, that they do not need to have our knowledge. Whenever they disclose anything to us, this is always a source of a potential leak of magnitude because it is outside of their control. And although we try very conscientiously, we also are greatly concerned that we are entrusted with this information which theoretically at least is of such vital importance to the Nation as to warrant warrantless tap.

Now, I have heard Mr. Petersen, for example, if I may allude to him, discuss the sensitivity of numbers and therefore I am moving with a certain amount of circumspection, but I would like to point out that he mentioned that there were approximately 100 wiretaps in 1973, but he could not give you the precise figure. Our figures, and I had them collated purely because of the fact that I was coming before the committee and normally we do not keep any centralized records, and again it is to protect maximum security, but I have been down this year. My number is significantly below that figure, which indicates that at least a number of taps were performed that could have been performed without our knowledge or——

Mr. KASTENMEIER. Or they, in fact, may not have used the telephone as a device.

Mr. CAMING. Yes. It could be an eavesdropping device. And we normally would not know about that and unless there is a court directive as part of our very restrictive policies, to do it voluntarily, and in the other 15 States which do not have a court directive, of the 22 States that have an enacted State enabling laws, we refuse to cooperate when the court order refers to eavesdropping alone, feeling that it is not, you know, a part of our network that is directly involved, although we recognize there is some tangential assistance obtained, if they can also run the eavesdrop through the network to a distant location.

Mr. DRINAN. Mr. Chairman?

Mr. KASTENMEIER. I yield to the gentleman from Massachusetts.

Mr. DRINAN. Could I come back to the point that even though there is no centralized figure, you were able to pull together a figure that you say is substantially under 100. Do I understand rightly that you do, in fact, keep all of these letters or authorizations, and

that the corporate officer responsible for security does, in fact, possess these at some particular place?

Mr. CAMING. Yes, Mr. Drinan. Each company, and it was not a very difficult task for me to get these figures, we just have no reason to keep them at headquarters. Each company has been told to keep the national security letters, no accompanying records or anything, but just the letters themselves permanently or indefinitely. We also keep, for your information, information with respect to cooperation in wiretaps under title III or the equivalent State law for a period of 10 years, which tracks with the period set forth in section 2518(8) of title III for court orders and applications. So, we keep any accompanying records.

Mr. KASTENMEIER. I am reassured on that point. Was it not one of your competitors who notoriously reverted to a paper shredder at one point in some case in the last few years?

Mr. CAMING. Let me point out here that I have been accused of working for I.T. & T. merely because there was a confusion of terminology within the United States with the perception of, I guess, litigation that may now develop which may now make them a competitor and they have normally operated only in the overseas theater. So, there was never any question prior to a Satellite application now being entertained of cooperation. We do cooperate with independent companies when necessary of the telephone industry, like General Telephone, to the extent of insurance that any cooperation we extend does not unfold at some other point. In other words, but generally speaking, no, most of our coperation is in the sense that when they come to our company, that is all that they desire, and if they come to an independent company, because their territory is being served they normally would have no reason to have recourse to us.

Mr. KASTENMEIER. I think I am correct in assuming, Mr. Caming, am I not, that American Telephone & Telegraph would experience the major impact of wiretapping and electronic eavesdropping under title III as opposed to other telephone companies?

Mr. CAMING. I think that would be very fair to say and conclude for several reasons. The first, of course, that from 80 to 85 percent of all of the phones in the United States at this time, certainly in the message toll network are Bell System phones.

Many of the principal centers of an urban character, where Crime seems to emanate, like New York or New Orleans or Los Angeles or Chicago or Washington, are served by our companies principally, so that most of the wiretaps would probably be requested there.

Mr. KASTENMEIER. May I pursue another line of questioning?

Mr. CAMING. Surely.

Mr. KASTENMEIER. And then I will yield to my friend from Massachusetts.

Are you or have you in the past, other than the leasing of lines which you alluded to briefly, been compensated by government agencies or law enforcement authorities for your cooperation? Have you ever considered to what extent, both in manpower and resources, the company ought to cooperate with agencies in conducting sur-

veillance? And have you considered whether there was a legal requirement that A.T. & T. cooperate with the installation of these devices?

Mr. CAMING. Of course, that is a subject dear to our hearts, as you can well imagine. First, we, of course, in the Federal area, have no longer cooperated in title III wiretapping, except under the court directive provision of 2518, and there any technical assistance or facilities provided are at the prevailing tariff rate, as expressly said in the Statute. We have taken the position also, I might say, that outside of the scope, the narrow scope of title III, that any cooperation on our part in any area, although lawful, is not mandated by the Congress and that we would, therefore, respectfully decline to cooperate in many situations.

For example, we do not engage in line identification, so-called tracing, even if the Government is operating under a title III court order. We have refused to trace lines because, not from the expense standpoint alone although that is an element, but our primary reason is that our general concern for privacy of communications compels us to the conclusion that we should restrict our activities to the degree that Congress and States under enabling legislation feel is wise for us to participate in, generally apart from the national security area, where there has been some expression. So, we do not engage, I might say, in a number of activities.

Now, other activities such as servicing title III orders for cable information, it is very difficult to calculate that there is any significant cost to us. If we have any cost to us. If we have any costs, such as providing a private line channel and having to do any engineering on it, occasionally to compensate for losses of transmission if the channel is over a certain distance, or we sometimes put in what we call dial impulse repeaters so that the dial impulses will come through clearly and not be lost in transmission, or that there is no sagging of transmissions, and someone says, uh, huh, my line must be wiretapped, those charges are put into our private line charges to the Government. And any charges under national security, I mean—I am sorry, any services provided under national security which we provide as channels, terminal to terminal, are also compensated for fully. We do as best as we can estimate our costs and do charge.

Mr. KASTENMEIER. And are those charges made openly or are they concealed? Are they made to the Department of Justice or just the General Services Administration or some other branch of Government?

Mr. CAMING. Surely now, starting with the premise that what they are doing is lawful, be it covert in the sense that the parties being overheard are not to know of it, and, thirdly, that it is court ordered, we are, or have molded our billing practices to the desires of the Government. We frequently bill to a fictitious name, or to a post office so that if you picked up the bill it would look like perhaps the ABC Toy Co., and if you just happened to see it in accounting also. We often have our billing done through security and they may keep the bills in order to maximize the security of the operation. But,

we will do it to a fictional address if they so request. In fact, we will do this for any subscriber if he asks, and his name is Smith and he asks us to bill it to the Jones Publishing Co., assuming that we have no knowledge of any impropriety in such request, we would normally bill as requested.

Mr. KASTENMEIER. Am I correct in assuming since 1969, that your subscriber in that connection has been the Department of Justice, or the FBI however otherwise billed? You do not have, I take it, White House, CIA, or other sources of requests that have not, in fact, gone through the Department of Justice or the Federal Bureau of Investigation? Is that correct?

Mr. CAMING. Assuming we are talking in the area of national security, the answer is unequivocably we only deal with the Department of Justice and the FBI. We have had no requests, to my knowledge, in that area, and we do not even make any particular—well, if we did receive such a request, we would immediately contact the Department of Justice about it. To my knowledge, it has always been my conception and it is limited, intelligence activities within the United States supposedly are to be confined to the Federal Bureau and we act upon that.

We do have, of course, the normal communication services with the White House, the CIA and, of course, these would be the normal provision of service to any customer.

Mr. KASTENMEIER. Yes, of course. I understand that.

One last line of questions. On page 10 of your statement you indicated that eavesdrop devices, lawful and unlawful, are found on company lines at an average of 21 a month. What percentage are unlawful?

Mr. CAMING. To tell you the truth, Mr. Kastenmeier, the number has always been so infinitestimal that we have never attempted to break it out. I was just looking through because I thought it might be of interest to the committee. That figure I gave of 21, being a lawyer and not really advanced in mathematics, and several of my college teachers could affirm that, I worked on the basis of the highest figure but actually the figure has turned out to be lower than that. Last year, for example, with 163 throughout the Bell System of devices of any type, lawful or unlawful, that we have discovered. The prior year was 174 and, in fact, since 1967, because I thought it would give the committee a better feel of it, if I may, and I am sure Mr. Lehman can take these down. 1967 we estimate we found 195 devices in all 24 of our companies aggregated of all types. 179 in 1968, 218 in 1969, 195 in 1970, 249 in 1971, which explains my high figure. One hundred seventy-four and then 163. So, because they have been so small and often—we are never quite certain on those devices whether they are lawful or unlawful, because some of those may be lawful, but once they are discovered the law enforcement authorities say, you know, well, we do not know anything about them and remember, too, that all of the State and local authorities in 22 States have the right to engage in wiretapping. So, we have never broken out a percentage of that minuscule amount out of the 138 million telephones, just giving a proportion.

Mr. KASTENMEIER. Do you have a procedure for reporting these, a portion of which would be unlawful presumably and a portion of which would be lawful to the law enforcement authorities?

Mr. CAMING. As I just alluded to in our statement, we report all cases because even if we find a device and have a court order on file, unless there was a little thing which was placed here by the New York State Police Department or the Boston Police Department, we would not know whether it was a coincidence, or whether this was actually a lawful device. It could be that more than one party is tapping the same line.

Mr. KASTENMEIER. In the case of what would be assumed to be unlawful bugs, and you may not know whether they are, have you found the Department of Justice responsive in investigating these cases? Certainly, the unlawful bugs are a menace to your subscribers, and are unwanted by you as a company and presumably you would like to see title II enforced.

Mr. CAMING. I would like to make a comment which probably means I have arrived at a position that I can make comments on my own. As I say, I have personally cooperated in overseeing this program for some 9 years. The Department of Justice, that I deal with is the Criminal Division, and very frequently the organized crime and racketeering groups which has oversight over title III and we do not get into national security very much, as you could see. It is not necessary. But, throughout from the inception in 1968 and the passage of title III the Criminal Division, under Mr. Petersen, has been aware of our concern, of the encroachments on privacy that title III made, and the fact that we do all necessary to effectuate the particular requests, but give them the minimum assistance and he has, and his staff has respected this, although they have disagreed on a number of occasions, such as with our recent measure in further restricting toll billing records. But we have, for instance, discussed at the time of the passage in February 1971 of the directive amendments to title III, which put us in the position of having to respond to a court order, which could direct us to do things, we said, and I said it personally, that it would be best to maximize privacy if they used only the statutory language in their court orders and we would then do the very minimum amount necessary and insure that the title III tap would be effectuated. But, in as restrictive a way as possible. I would say to that, that whenever we have brought their attention to any questions of the nature you address on wiretapping that they have been utterly responsive and utterly cooperative and, in fact, I think that some of their task forces in the field have complained at times that they were too solicitous.

Mr. KASTENMEIER. I appreciate that response, although there is some concern, and I shall it, that generally speaking, the Justice Department, is not pursuing prosecutions under title III.

Mr. CAMING. I see.

Mr. KASTENMEIER. To dissuade people, in some cases unauthorized Government officials, from engaging in these practices.

Mr. CAMING. I can appreciate that. My remarks were addressed to what I thought was your earlier statement as to their general attitude with respect to our procedures, when we find a device, whether

lawful or unlawful. If it is a lawful device, as far as it appears, by our having a court order, we would then contact the agency concerned and if it is a State agency or the FBI, we would contact them. Now if it was an unlawful device, we would contact first the Federal, local agency, remembering it is our local telephone company that finds it in each case and we contact the local agency of the FBI. And, in addition, we contact the appropriate local authority whether it is the State or the county or a city, and we have the coordinates to do that *with, because the Federal authorities might say this is unlawful and* we do not know that that is a lawful tap, and it might turn out to be a State or a local tap, so we contact both. Then if they both declare or all parties declare that they do not know of it being lawful, we then say we intend to remove it and keep it under surveillance, and if it is trouble-inducing, we immediately disable it anyway, but, we leave it in place. But, we will if you wish permit you 24 to 48 hours, and I do know at least in a number of cases, the ones I think happened to be with State police or local police, where they have actually undertaken a surveillance, and then, if within a reasonable period it proves fruitless, we really remove the device.

Now, if they do not want to investigate we, in some of our companies, attempt, because it is rather difficult to investigate this source. Our main concern is if you just remove the device but do not apprehend the wiretapper, it is virtually like picking up some burglary tools but leaving the burglar free. So, we do cooperate but usually only to the extent of 48 hours and the customer is advised that an unlawful device has been found.

Mr. KASTENMEIER. Thank you.

I yield to the gentleman from Massachusetts.

Mr. DRINAN. Thank you, Mr. Chairman, and thank you, Mr. Caming. This is very, very informative. I have listened here fascinated at all of your problems.

Let me try to clarify something for myself.

Mr. CAMING. Surely.

Dr. DRINAN. If the Department of Justice puts a tap on, unbeknownst to the A.T. & T. and unbeknownst to the subscriber, would that be illegal?

Mr. CAMING. In my opinion, if it were not it the area of national Security and I could not pass the comment upon the legality, but assuming arguendo the legality of that type of tap, apart from that, it is clearly——

Mr. DRINAN. Assuming——

Mr. CAMING. I am sorry. If they place a tap on the line without our knowledge but have a valid court order, for example, we have argued among ourselves with the company, what is this, and it seems that it is not a technical trespass on the ground that it is court authorized. In fact, some State statutes have expressed it but assuming there is no title III, I would say this: That the Department of Justice or any other branch of Government, Federal or State or local, is just as liable under the proscriptions of title III.

Mr. DRINAN. Therefore, since your figures show substantially less than 100 wiretaps, we can make an inference that the Department of Justice is, in fact, engaging in warrantless wiretaps without the

knowledge or consent of the A.T. & T. If one of those taps were discovered, what would the A.T. & T. do?

Mr. CAMING. OK. Now, perhaps in my attempt to say substantially, or perhaps the term significantly would be—but if we discovered a national security device, Mr. Drinan, first there may be some serious question whether we would know that it is that. They would have to tell us about it.

Mr. DRINAN. Let me back up. That just tells us about the practice. How easy is it for this never to be discovered? It is conceivable that they could have dozens or even hundreds of them now, and that in the nature of things they would never be discovered?

Mr. CAMING. Well, the sophistication and technology today, the continual advances, it is very difficult in certain areas, such as inductively couple devices, which may not be actually touching our line, and our people are instructed to be constantly on the alert—for example, any installer or repairman that goes in normally would check over the facility. However, if they had concealed them at some distant point, it is conceivable, at least, if it is well done, that neither we nor the subscriber would be aware of it.

Mr. DRINAN. But coming back to my original question, I am not certain that I got that clear, as to what would the A.T. & T. do if it did discover a warrantless tap placed there by the Department of Justice?

Mr. CAMING. Well, all right. Well, the first thing would be that we would discover the device. We would not know at the moment what it was. If it was discovered as a result of a customer complaint, it would probably have been found by our security forces, or plant forces, under their direction, checking out the complaint, or it could have been stumbled upon by a repairman or installer. And in that case it is required that any employee do nothing but report it immediately through his lines of supervision to Security.

Mr. DRINAN. All right. All of that has gone by. I am asking——

Mr. CAMING. They would then go to the Government.

Mr. DRINAN. And they admit openly, yes, we did it, and we are sorry you discovered it?

Mr. CAMING. In that case, we would leave the tap in place, I would assume.

Mr. DRINAN. Yes. Why? This is a trespass. This is illegal. Why do you do that? You are cooperating in evil, now.

Mr. CAMING. Well, no, I guess we may be misunderstanding each other because I certainly would not say we are cooperating in evil. I guess I did not understand your question. I was assuming that they said the following to us: This is a national security tap. It is in a very sensitive area. It has been expressly authorized by the Attorney General and if you wish, we will give you the proof. We did not wish to bring this to your attention in order to maximize the security of the operations, and we wish you would leave it in place. In that case, assuming we have no customer complaint, for example, we would probably do so if we had the necessary proof adduced. In other words, if we got a national security letter saying yes, this was, and we did not desire it, there is no reason for the Government to bring

it to our attention in national security taps and that is lawfully put on by them.

Mr. DRINAN. Would the subscriber in such a situation have a claim against the A.T. & T. because they had allowed his wire to be tapped unbeknownst to him?

Mr. CAMING. Well, you mean after the discovery when it was continued? No more so than if *ab initia* we had received a letter request, assuming the same situation. And we have established after discovery that it is a national security tap.

Mr. DRINAN. This is a pretty permissive attitude on your part to allow the Department of Justice to give you a letter any time they want. In other words, you are really not demanding a letter ahead of time.

Mr. CAMING. Oh, no.

Mr. DRINAN. You are not really?

Mr. CAMING. We are in a position almost as a stakeholder, Mr. Drinan. We are required to venture into areas that are quite foreign to us. We do not wish to participate in any of this any further than the Congress, and the necessity of the situation warrants. I can assure you of that. When we get a letter from the Director or from the Attorney General, we have no knowledge other than the facial letter of the validity of the contention. We merely assume that a man of that stature in the Government, and we have no alternative, but to assume that he would not——

Mr. DRINAN. But legally, you could refuse to cooperate?

Mr. CAMING. Yes, I think we could.

Mr. DRINAN. Has it been considered at the highest level that maybe the A.T. & T. should refuse to collaborate in warrantless taps?

Mr. CAMING. I think it is fair to say that that has been considered ever since the inception in 1941, as of necessity, that it was recognized that frequently our assistance may be almost indispensible to effectuate a wiretap. The number of requests have never over the years been at such volume to——

Mr. DRINAN. That is immaterial if it violates the fourth amendment.

Mr. CAMING. I agree with that, and am not talking about that aspect. We have always had recognition, you might say from the Congress, when we testified in 1966 and 1967, we brought the National security question to the attention of Congress in our testimony. In 2511.3 of 18 United States Code, the Congress, and in its underlying Senate Report 1097 of April 1968, took cognizance of the importance of the national security and its constitutional significance. These are only guideposts.

Mr. DRINAN. And they did not require you to cooperate. The Congress did not require you to cooperate.

Mr. CAMING. No, the Congress did not require us to cooperate.

Mr. DRINAN. That is right. You are free agents. Has the Board of Directors of A.T. & T. ever been given the question of whether they will cooperate in warrantless taps?

Mr. CAMING. I think we could take that legal position.

Mr. DRINAN. I am asking you why has not the A.T. & T. ever gone above management with this question? Has it ever gone to the policy

directors of this very public company that has 150 million subscribers?

Mr. CAMING. I am sorry, I did not catch the point. Has it ever gone ahead——

Mr. DRINAN. Above the management level? Has it ever gone to the Board?

Mr. CAMING. I would say that we have received, in fact we reviewed recently before the board of directors our policy in wiretapping generally. Our vice president then of operations and now of customer services did review with our board our policy. Now, whether that included national security matters I cannot say with certainty, not having been present. It is my opinion that they were generally aware of it, and of the circumscribed areas in which we cooperate. Now, we do not cooperate in internal security matters now as we would define that term, only to the extent that the letter spells out the foreign intelligence areas set forth in my statement.

Mr. DRINAN. I asked these questions, Mr. Caming, because I was very impressed with your testimony. And as you heard, we are not getting very much cooperation from the Department of Justice, and perhaps the only way to protect the privacy of the people on their phone lines in America, is to have the telephone company do what it is authorized to do; namely, refuse to cooperate unless wiretapping is done pursuant to law. So that is a new avenue that has been opened up to me by your testimony, and for that I am grateful.

I would ask this, sir, in conclusion, that if you have any subsequent answers that you would like to give or a more complete explanation of some of these questions that came up, I know that your testimony would be very helpful and you could submit further statements.

Mr. CAMING. Thank you, Mr. Drinan. I might also say that I would like to express our appreciation for being given the opportunity to appear. And we are completely at the disposal of the subcommittee, and we have had some very fine relationships with Mr. Lehman preliminarily and we will do anything to assist the subcommittee in its deliberations, and will be pleased to hear from you.

Mr. DRINAN. Thank you very much.

[The prepared statement of Mr. Caming follows:]

STATEMENT OF H. W. WILLIAM CAMING, ATTORNEY, AMERICAN TELEPHONE & TELEGRAPH CO.

I am H. W. William Caming, Attorney in the General Departments of American Telephone and Telegraph Company. My areas of primary responsibility have since 1965 included, from a legal standpoint, oversight over matters pertaining to industrial security and privacy as they affect the Bell System.

I wish to thank the Subcommittee for the opportunity to present the views of the Bell System on privacy of communications and delineate our experiences with electronic surveillance, principally in the area of wiretapping.

At the outset, I wish to stress the singular importance the Bell System has always placed upon preserving the privacy of telephone communications. Such privacy is a basic concept in our business. We believe that our customers have an inherent right to feel that they can use the telephone with the same degree of privacy they enjoy when talking face to face. Any undermining of this confidence would seriously impair the usefulness and value of telephone communications.

Over the years, the Bell System has repeatedly urged that full protection be accorded to its customers' privacy, and we have consistently endorsed legislation that would make wiretapping as such illegal. In 1966 and again in 1967,

we testified to this effect before the Senate Subcommittee on Administrative Practice and Procedure during its consideration of the Federal Omnibus Crime Control and Safe Streets Bill. We said we strongly opposed any invasion of the privacy of communications by wiretapping and accordingly welcomed Federal and State legislation which would strengthen such privacy. This is still, of course, our position.

We believe that the Federal Omnibus Crime Control Act has contributed significantly to protecting privacy by, among others, clarifying existing law and proscribing under pain of heavy criminal penalty any unauthorized interception "or" disclosure or use of a wire communication.

During our Congressional testimony, we said too that we recognized that national security and organized racketeering are matters of grave concern to the government and to all of us as good citizens. The extent to which privacy of communications should yield and where the line between privacy and police powers should be drawn in the public interest are matters of national public policy, to be determined by the Congress upon a proper balancing of the individual and societal considerations.

For more than three decades, it has been Bell System policy to refuse to accept in the Yellow Pages of its telephone directories advertisements by private detective agencies and others, stating or implying that the services being offered include the use of wiretapping. In December 1966, during Congressional consideration of the Federal Omnibus Crime Control Act's Title III proscriptions against unauthorized interceptions, this longstanding policy was expanded to prohibit too the acceptance of eavesdropping copy. This standard, adopted by all Bell System Companies, was interpreted from the outset to make equally unacceptable so-called debugging advertising (*i.e.*, advertising stating or implying electronic devices or services will be provided for the detection and removal of wiretaps and eavesdropping "bugs"), on the theory that those who can debug also possess the capability to bug and wiretap.

Our Companies continually review their Yellow Pages in an endeavor to ensure all unacceptable copy is removed, either by satisfactory rewording or deletion of the offending copy. New advertising is subject to similar scrutiny. The scope of this undertaking becomes apparent from the fact that there are approximately 2,400 Yellow Pages telephone directories, containing some 18,000,000 advertisements and listings.

The removal of unacceptable copy is a neverending task of large proportions, since many such advertisements are revised, and new ones appear, in each issue. We believe, however, that we have done a creditable job in this area, and we intend to continue such rigid policing as contributive to maximizing privacy of communications.

It may help place matters in perspective if we provide a brief insight into the magnitude of telephone calling that occurs in this country in a single year. During the calendar year 1973, for example, there were approximately 138 million telephones (including extensions) in use in the United States, from which some 188 billion calls were completed.

From the time our business began some 90 years ago, the American public has understood that the telephone service they were receiving was being personally furnished by switchboard operators, telephone installers and central office repairmen who, in the performance of their duties of completing calls, installing phones and maintaining equipment, must of necessity have access to customers' lines to carry out their normal job functions. We have always recognized this and have worked hard and effectively to ensure that unwarranted intrusions on customers' telephone conversations do not occur. We are confident that we have done and are doing an excellent job in preserving privacy in telephone communication.

The advance of telephone technology has in itself produced an increasing measure of protection for telephone users. Today, the vast majority of calls are dialed by the customer, without the presence of an operator on the connection. This has greatly minimized the opportunities for intrusions on privacy. In addition, more than 88 percent of our customers now have one-party telephone service, and the proportion of such individual lines is growing steadily. Direct inward dialing to PB– extensions, automatic testing equipment, and the extension of direct distance dialing to person-to-person, collect and credit card calls and to long distance calls from coin box telephones further contributes to telephone privacy.

Beyond this, all Bell System Companies conduct a vigorous program to ensure every reasonable precaution is taken to preserve privacy of communications through physical protection of telephone plant and thorough instruction of employees.

Our employees are selected, trained, and supervised with care. They are regularly reminded that, as a basic condition of employment, they must strictly adhere to Company rules and applicable laws against unauthorized interception or disclosure of customers' conversations. All employees are required to read a booklet describing what is expected of them in the area of secrecy of communications. Violations can lead, and indeed have led, to discharge.

In regard to our operating plant, all of our premises housing central offices, equipment and wiring and the plant records of our facilities, including those serving each customer, are at all times kept locked or supervised by responsible management personnel, to deny unauthorized persons access thereto or specific knowledge thereof. We have some 90,000 people whose daily work assignments are in the outside plant. They are constantly alert for unauthorized connections or indications that telephone terminals or equipment have been tampered with. Telephone cables are protected against intrusion. They are fully sealed and generally filled with gas; any break in the cable sheath reduces the gas pressure and activates an alarm.

With these measures and many others, we maintain security at a high level. We are, of course, concerned that as a result of technological developments, clandestine electronic monitoring of telephone lines by outsiders can be done today in a much more sophisticated manner than has been heretofore possible. Devices, for example, now can pick up conversations without being physically connected to telephone lines. These devices must, however, generally be in close proximity to a telephone line, and our personnel in their day-to-day work assignments are alert for signs of this type of wiretapping too. Every indication of irregularity is promptly and thoroughly investigated.

Our concern for the privacy of our customers is reflected too in the care with which we investigate any suspicious circumstances and all customer complaints that their lines are being wiretapped. Our Companies follow generally similar operating procedures when an employee discovers a wiretap or eavesdropping device on a telephone line. Each Company has established ground rules for the small number of these situations that occur, which take into consideration any local statutory requirements. Most frequently, when our people find improper wiring at a terminal, it is the result either of a record error or failure on the part of our personnel to remove the wires associated with a disconnected telephone. Each of these cases is, however, carefully checked. In those few instances where there is evidence of wiretapping, the employee discovering it is required to inform his supervisor immediately, and a thorough investigation is undertaken in every such case by competent security and plant forces.

In a small number of cases, a customer suspects a wiretap and asks for our assistance. Usually, these requests arise because the customer hears what are to him suspicious noises on his line. Hearing fragments of another conversation due to a defective cable, or tapping noises due to loose connections, or other plant troubles are on occasion mistaken for wiretapping. Each Company has established procedures for handling such requests. Generally, the first step is to have our craftsmen test the customer's line from the central office. In most instances, these tests will disclose a plant trouble condition. In each such case, the trouble is promptly corrected and the customer informed there was no wiretap.

In cases where no trouble is detected through testing the customer's line, a thorough physical inspection for evidence of a wiretap is made by trained personnel at the customer's premises and at all other locations where his circuitry might be exposed to a wiretap. If no evidence of a wiretap is found, the customer is so informed. Where evidence of a wiretap is found, the practice generally is to report to law enforcement authorities any device found in the course of the Company inspection, for the purposes of determining whether the device was lawful and of affording law enforcement an opportunity to investigate if the tap was unlawful. The existence of the device is also reported to the customer requesting the check, generally irrespective of whether it was lawful or unlawful. The customer is told that "a device" has been found on his line, without our characterizing it as lawful or unlawful; should the customer have any questions, he is referred without further comment to law enforcement.

New Jersey Bell, however, as a matter of policy, informs a customer requesting a wiretap check that only the presence of an unauthorized device will be disclosed. Minnesota by statute similarly limits disclosure to unlawful devices. Should the customer inquire about the presence of a lawful device, he will usually be assured that applicable Federal and State laws require any judge authorizing or approving a court-ordered interception to notify the affected customer within 90 days after interception ceases (or at a later date, if disclosure is postponed upon a good cause showing by law enforcement).

All Bell System Companies report the existence of an unlawful device to the customer requesting the check, as well as to law enforcement, and the latter is provided an opportunity to investigate for a reasonable period (generally 24–48 hours) prior to removal of the wiretap.

We might point out that unless the wiretap effort is amateurish, a person whose line is being tapped will not hear anything unusual, because of the sophisticated devices employed. As we previously said, most of the complaints originate because the customer hears an odd noise, static, clicking, or other unusual manifestations. As far as our experience discloses, these usually turn out to be difficulties in transmission or other plant irregularities. From 1967 onward, for example, the total number of wiretap and eavesdrop devices of all types (including both lawful and unlawful) found by telephone employees on Bell System lines has averaged less than 21 per month—an average of less than one a month for each of the twenty-four operating companies of the Bell System. In our opinion, the criminal sanctions imposed by Title III (for the unauthorized interception or disclosure or use of wire or oral communications, or the manufacture, distribution, possession, or advertising of intercepting devices), coupled with vigorous law enforcement and attendant publicity, appear to have contributed significantly to safeguarding telephone privacy.

In the area of court-ordered wiretapping, it is the policy of the Bell System to cooperate with duly authorized law enforcement authorities in their execution of lawful interceptions by providing limited assistance as necessary for law enforcement to effectuate the particular wiretap. We wish to stress that the Bell System does not do the wiretapping. The assistance furnished generally takes the form of providing line access information, upon the presentation of a court order valid on its face, as to the cable and pair designations and multiple appearances of the terminals of the specific telephone lines approved for interception in the court order.

The term "cable and pair" denotes the pair of wires serving the telephone line in question, and the cable (carried on poles, or in conduit, or buried in the earth) in which the pair reposes. A "terminal" is the distribution point to which a number of individual pairs of wires from the cable are connected, to provide service in that immediate area. A terminal may in a residential area be on aerial cable suspended from telephone poles or on a low, above-ground pedestal, or be found in terminal boxes or connecting strips in the basement, hall, or room of an office building or apartment house. The pair of wires of each telephone serviced from a particular terminal are interconnected at that terminal with a specific pair of wires from the cable, so that a continuous path of communication is established between the customer's premises and the telephone company's central office. The terminals vary in size, depending upon the needs of the particular location. To provide optimum flexibility in usage of telephone equipment, the same pair of wires may appear in parallel in a number of terminals, so that the pair can be used to service a nearby location if its use is not required at a particular point. Thus, the term "multiple appearance" denotes the locations where the same pair of wires appears in more than one terminal on the electrical path between the central office and the customer's premises.

In the instance of law enforcement authorities of the Federal government (and of those States enacting specific enabling legislation in conformity with the amendments to § 2518(4) of Title III of the Federal Omnibus Crime Control Act effective February 1, 1971), the court order may "direct" the telephone company to provide limited assistance in the form of the "information, facilities, and technical assistance" necessary to accomplish the wiretap unobtrusively and with a minimum disruption of service. Upon the receipt of such a directive in a court order valid on its face, our cooperation will usually take the form of furnishing a private line channel from terminal to terminal (*i.e.*, a channel from a terminal which also services the telephone line under investiga-

tion to a terminal servicing the listening post location designated by law enforcement). Additionally, the above described line access information will be furnished for the specific telephone lines judicially approved for interception.

On occasion, assistance in the form of private line channels is furnished to Federal authorities in national security cases. This assistance is only rendered upon specific written request of the Attorney General of the United States or of the Director of the Federal Bureau of Investigation (upon the specific written authorization of the Attorney General to make such request) to the local telephone company for such facilities, as a necessary investigative technique under the Presidential power to protect the national security against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. For reasons of security, we are not informed in such cases of the specific nature of the national security matter under investigation.

In cooperating in court-ordered and national security cases, we endeavor to provide the very minimum assistance necessary to effectuate the particular wiretap. Under no circumstance, do we do the wiretapping itself; that is the exclusive province of the appropriate law enforcement officers. Nor do we furnish end equipment to be used in connection with a wiretap, such as tape recorders or pen registers. Nor do we design or build wiretap or eavesdrop devices for law enforcement authorities. Furthermore, our telephone companies do not train law enforcement personnel in the general methods of wiretapping and eavesdropping, nor do we provide telephone company employee identification cards, uniforms or tools, or tlephone company trucks.

In conclusion, I wish to assure you that the Bell System continues to be wholly dedicated to the proposition that the public is entitled to telephone communications free from unlawful interception or divulgence. We are vitally interested in the protection of the privacy of communications and always welcome measures and techniques that will strengthen and preserve it.

The foregoing reflects our experience in the areas of wiretapping and electronic surveillance since the passage of Title III of the Federal Omnibus Crime Control Act in 1968 and our continuing concern for maximizing the privacy of communications.

I shall be pleased to endeavor to answer any questions that the Subcommittee may have.

Mr. DRINAN. I would like to announce the hearings on eavesdropping and electronic surveillance will continue in this room on Monday, April 27. We will hear from a representative of the FBI, Professor William Bender of Rutgers University, and Representative Bella Abzug.

The meeting is adjourned. Thank you.

[Whereupon, at 1:45 the hearing was recessed to reconvene on Monday, April 29, 1974, at 10 a.m.]

WIRETAPPING AND ELECTRONIC SURVEILLANCE

MONDAY, APRIL 29, 1974

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES,
AND THE ADMINISTRATION OF JUSTICE OF THE
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The subcommittee met at 10:15 a.m., pursuant to recess, in room 2141, Rayburn House Office Building, Hon. Robert W. Kastenmeier (chairman) presiding.

Present: Representatives Kastenmeier Drinan, Smith, and Cohen.

Also present: Bruce A. Lehman, Counsel, and Thomas E. Mooney, associate counsel.

Mr. KASTENMEIER. The subcommittee will come to order this morning to hear further testimony relating to wiretapping and electronic surveillance.

We are very pleased to welcome our first witness this morning, Mr. Edward S. Miller, appearing on behalf of the Federal Bureau of Investigation as Deputy Associate Director. Mr. Miller is in charge of all of the investigative activities of the Bureau in both the criminal and national security areas.

Before proceeding, I should explain that the Chair recognizes that Mr. Miller is under some limitations in discussing publicly some aspects of national security electronic surveillance. He may, therefore, be unable to respond specifically to certain questions as the Chair understands it.

I might ask you to identify your colleagues, Mr. Cleveland and Mr. Decker, and to proceed sir. We have your extensive statement. If you desire you may read the entire statement or present an oral summary, whichever you choose.

TESTIMONY OF EDWARD S. MILLER, DEPUTY ASSOCIATE DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, ACCOMPANIED BY WILLIAM V. CLEVELAND, ASSISTANT DIRECTOR, SPECIAL INVESTIGATIVE DIVISION; ANDREW J. DECKER, JR., INSPECTOR, INTELLIGENCE DIVISION

Mr. MILLER. Thank you, Mr. Chairman.

Before I begin, I will introduce my Colleagues, Assistant Director William Cleveland, who is in charge of what we call our Special Investigative Division. One of its primary tasks is conducting investigations in the organized crime field.

Mr. Decker, on my right, is the inspector in charge of our counter-intelligence in the Intelligence Division.

I will read excerpts from my statement—some six pages.

Mr. Chairman and members of the subcommittee, the gist of the bills before this subcommittee is aimed at either prohibiting all types of electronic surveillance, including those which Congress has already considered and found desirable, or at perceived actual or potential abuses of electronic surveillance. One bill, H.R. 13825, attempts to define and regulate the use of electronic surveillance by the President in cases in which only he may have authority to act under his constitutional powers.

In 1968, Congress decided that electronic surveillances provided an effective, and in some cases, indispensable law enforcement tool in the investigation of certain crimes. Congress provided that a commission would study the effect of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 6 years after implementation and within 1 year report its findings to the Congress. If corrective or remedial action appears necessary, Congress will then have extensive and objective data upon which to base further action. The commission has been fully appointed and will begin its study this year.

Any amendment to title III should await the results of the commission's study, which will reflect both the value of electronic surveillance in modern law enforcement, and the measures and difficulties in protecting individual rights while utilizing this investigative technique.

I, like all of you, am concerned with the abuses of electronic surveillance. Abuses redound to the detriment of the legitimate, fair and effective use of electronic surveillance as a valuable tool against criminal activity and foreign intelligence operations.

Some would seek to outlaw the use of electronic surveillances in all cases, perhaps based on the fact that electronic surveillance is not sufficiently selective and often intercepts many communications not directly pertaining to the matter under investigation. This is often true, but in many cases it is not true. Use of electronic surveillance involves a delicate balancing of protecting the common good against individual rights. While some communications are intercepted which are extraneous to the offense which justifies the surveillance, evidence of the communications which form part of the offense cannot generally be obtained in any other way; consequently, many crimes would go undetected and unprosecuted without the use of electronic surveillances. In many cases electronic surveillances intercept no extraneous communications, for example, listening in to kidnapers' or extortionists' telephone calls, and the use of a body recorder by an undercover agent or informant.

The use of electronic surveillance in foreign intelligence cases is an absolutely essential and indispensable tool. Information of much value beyond neutralization is obtained in such cases.

While the Congress certainly should direct itself to abuses of electronic surveillance, it hopefully will include in its deliberation the effect such legislation might have on the practical necessities of criminal and intelligence investigations. For that reason, I welcome the opportunity to appear before you today to present my views on

the bills pending before this subcommittee on the proper and improper use of electronic surveillances. I disagree with the complete abolition of electronic surveillance as an investigative tool, but I support measures to properly regulate and control its use.

There is a need for Congress to act, which need has been dramatized by recent cases, to provide for the use of electronic surveillance in criminal intelligence and domestic internal security investigations. The *Keith* case recognized that it was creating a void in the law by prohibiting the use of electronic surveillances in domestic internal security intelligence investigations by ruling that the President did not have inherent powers to authorize them without judicial warrant and invited Congress to consider procedures by which such surveillance could be obtained. The Court recognized that the standard of probable cause might be somewhat different in justifying the need for an intelligence electronic surveillance than the standard required under the current provisions of title III for criminal cases.

There is a need for domestic intelligence electronic surveillance in some cases in the United States today; however, there is no mechanism or procedure by which such surveillances can be utilized. We hope in the near future to present to Congress, following approval of the Department of Justice, a bill which will authorize the use of domestic intelligence electronic surveillances, with prior judicial approval, under reasonable probable cause, notice, and reporting requirements, suited to the legitimate objectives of intelligence investigations.

Mr. Chairman, I am confident that you and the members of the subcommittee are aware that I cannot discuss details of electronic surveillance in the national defense and foreign policy areas in open session.

Detailed discussion in these areas could possibly allow foreign intelligence services to assess the success of their operations and adjust their efforts or tactics to avoid neutralization and penetration.

Sensitive foreign policy and foreign relations considerations are also involved in any discussion of this nature.

Further, detailed discussion of the mechanics of electronic surveillance practices in the national defense, foreign policy, or organized crime areas, would be of inestimable value to the targets by perhaps enabling them to take countermeasures.

If the subcommittee feels it has a need for more detailed discussion in these areas, I would be most willing to meet with you in executive session.

My prepared testimony makes a case for the value of electronic surveillance in combating organized crime and provides an example of its effective use under the regulations of title III. Let me summarize that presentation merely by saying that organized crime is a highly sophisticated, far-flung, and pervasive evil influence in American life today. Much of its effectiveness, like any other organization's, depends on its communications capabilities. The telephone is an integral element in its success and without secure oral communications between leaders, superiors, and subordinates, it could not function. Title III has done much to neutralize the efficiency of organized crime. Any measure which would revoke the electronic surveil-

lance capability of law enforcement against organized crime would be a serious disservice to the American people.

My statement details, step-by-step, the manner by which a title III surveillance is requested, approved, implemented and regulated. I think you will find that the rights of the citizen are well protected against unreasonable government action and are provided a fair balancing against competing societal rights, both by the internal administrative procedures of the FBI and the Department of Justice, and an intervening judge.

My statement also contains some examples of the value of consensual monitoring, for example, monitoring of conversations with the consent of one party to the conversation. This technique is used significantly in organized crime cases in which perjury, intimidation, or murder of witnesses and destruction of evidence are not uncommon phenomena. A mechanical reproduction of a conversation and a law enforcement officer/witness who monitored the conversation have been indispensable to successful prosecution in several cases, and because there has been independent evidence of a conversation, the life of the party who consented to the monitoring who might otherwise have been the only witness, may have been saved.

As previously noted, consensual monitoring has assigned in not only solving kidnapings but may also have saved victims' lives.

I have also included in my prepared statement a detailed analysis of the bills pending before this subcommittee and the impact they could have on FBI operations.

Mr. Chairman, this concludes my oral statement.

Mr. KASTENMEIER. Thank you very much, Mr. Miller, it is a valuable statement indeed, and even though some of the testimony in your written statement was not delivered aloud, nonetheless, without objection, your full statement will be made a part of the record, and we appreciate having it.

[The statement of Mr. Edward S. Miller, Deputy Associate Director, Federal Bureau of Investigation, follows:]

STATEMENT OF EDWARD S. MILLER, DEPUTY ASSOCIATE DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Mr. Chairman and members of the Subcommittee, the gist of the bills before this Subcommittee is aimed at either prohibiting all types of electronic surveillance, including those which Congress has already considered and found desirable, or at perceived actual or potential abuses of electronic surveillance. One bill, H.R. 13825, attempts to define and regulate the use of electronic surveillance by the President in cases in which only he may have authority to act under his constitutional powers.

In 1968, Congress decided that electronic surveillances provide an effective, and in some cases, an indispensable law enforcement tool in the investigation of certain crimes. Congress provided that a commission would study the effect of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, six years after implementation, and within one year report its findings to the Congress. If corrective or remedial action appears necessary, Congress will then have extensive and objective data upon which to base further action. The commission has been fully appointed and will begin its study this year.

Any amendment to Title III should await the results of the commission's study which will reflect both the value of electronic surveillance in modern law enforcement, and the measures and difficulties in protecting individual rights while utilizing this investigative technique.

I, like all of you, am concerned with the abuses of electronic surveillance. Abuses redound to the detriment of the legitimate, fair and effective use of electronic surveillance as a valuable tool against criminal activity and foreign intelligence operations.

Some would seek to outlaw the use of electronic surveillances in all cases, perhaps based on the fact that electronic surveillance is not sufficiently selective, and often intercepts many communications not directly pertaining to the matter under investigation. This is often true; but in many cases, it is not true. Use of electronic surveillance involves a delicate balancing of protecting the common good against individual rights. While some communications are intercepted which are extraneous to the offense which justifies the surveillance, evidence of the communications which form part of the offense cannot generally be obtained in any other way; consequently, many crimes would go undetected and unprosecuted without use of electronic surveillances. In many cases electronic surveillances intercept no extraneous communications, e.g., listening in to kidnapers or extortionist's telephone calls, and the use of a body recorder by an undercover agent or informant.

The use of electronic surveillance in foreign intelligence cases is an absolutely essential and indispensable tool. Information of much value beyond neutralization is obtained in such cases.

While the Congress certainly should direct itself to abuses of electronic surveillance, it hopefully will include in its deliberation the effect such legislation might have on the practical necessities of criminal and intelligence investigations. For that reason, I welcome the opportunity to appear before you today to present my views on the bills pending before this Subcommittee on the proper and improper use of electronic surveillances. I disagree with the complete abolition of electronic surveillance as an investigative tool, but I support measures to properly regulate and control its use.

There is a need for Congress to act, which need has been dramatized by recent cases, to provide for the use of electronic surveillances in criminal intelligence and domestic internal security investigations. The Keith case recognized that it was creating a void in the law by prohibiting the use of electronic surveillances in domestic internal security intelligence investigations by ruling that the President did not have inherent powers to authorize them without judicial warrant, and invited Congress to consider procedures by which such surveillances could be obtained. The Court recognized that the standard of probable cause might be somewhat different in justifying the need for an intelligence electronic surveillance than the standard required under the current provisions of Title III for criminal cases.

There is a need for domestic intelligence electronic surveillance in some cases in the United States today; however, there is no mechanism or procedure by which such surveillances can be utilized. We hope in the near future to present to Congress, following approval of the Department of Justice, a bill which will authorize the use of domestic intelligence electronic surveillances, with prior judicial approval, under reasonable probable cause, notice, and reporting requirements suited to the legitimate objectives of intelligence investigations.

Mr. Chairman, I am confident that you and the members of the Subcommittee are aware that I cannot discuss details of electronic surveillance in the national defense and foreign policy areas in open session.

Detailed discussion in these areas could possibly allow foreign intelligence services to assess the success of their operations, and adjust their efforts or tactics to avoid neutralization and penetration.

Sensitive foreign policy and foreign relations considerations are also involved in any discussion of this nature.

Further, detailed discussion of the mechanics of electronic surveillance practices, in the national defense, foreign policy, or organized crime areas, would be of inestimable value to the targets by perhaps enabling them to take countermeasures.

If the Subcommittee feels it has a need for more detailed discussion in these areas, I would be most willing to meet you in executive session.

My prepared testimony makes a case for the value of electronic surveillance in combating organized crime and provides an example of its effective use, under the regulations of Title III. Let me summarize that presentation merely by saying that organized crime is a highly sophisticated, far-flung, and pervasive evil influence in American life today. Much of its effectiveness, like any

other organization's, depends on its communications capabilities. The telephone is an integral element in its success; and without secure oral communications between leaders and between superiors and subordinates it could not function. Title III has done much to neutralize the efficiency of organized crime. Any measure which wiuld revoke the electronic surveillance capability of law enforcement against organized crime would be a serious disservice to the American people.

TITLE III ELECTRONIC SURVEILLANCES

Title III electronic surveillances have been used against organized crime in investigations involving racketeer influenced and corrupt organizations; interstate transportation in aid of racketeering; interstate transmission of wagering information; illegal gambling businesses; and extortionate credit transactions. As a by-product, evidence was also developed concerning illegal narcotics traffic; prostitution; auto theft; alcohol, tobacco, and firearms tax violations; government corruption; stolen property violations ;and local robbery and gambling offenses. Title III surveillances have been used by the FBI in bribery; bank robbery; obstruction of justice; theft from interstate shipment; interstate transportation of stolen property, and kidnaping cases.

Title III has provided a most effective weapon in attacking syndicated gambling and other organized illegal activities. Since 1969, Title III electronic surveillances in FBI cases have led to over 1,100 convictions, and the confiscation of cash, property, weapons, wagering paraphernalia, and contraband valued at more than $7,000,000. Of approximately 2,700 organized crime subjects being prosecuted as of April 1, 1974, nearly 1,700 were arrested as a result of information obtained via Title III surveillances.

An example of the value of electronic surveillance is the DeCavalcante case:

Samuel Rizzo DeCavalcante, the head of an Elizabeth, New Jersey, mob allegedly engaged in gambling, loan sharking, extortion, labor-racketeering, and other illegal activities, had been the subject of an extensive FBI investigation for some time. In September, 1969, probable cause was established to indicate that DeCavalcante was involved with an individual named Alessio Barrasso in running one of the largest numbers operations in the State of New Jersey. A Title III surveillance on a key bet-taking telephone at Belleville, New Jersey, was authorized.

This coverage confirmed that DeCavalcante, Barrasso, and others were conducting a large-scale gambling business, and enabled us to obtain additional court orders authorizing telephone interceptions in New Jersey and Troy, New York. In December, 1969, DeCavalcante, Barrasso, and 53 others were indicted on conspiracy to violate Federal antigambling statutes, and eventually 49 of the 55 indicated pleaded guilty to the conspiracy charges.

Extensive investigation in this case, preceding the use of electronic surveillances, included five months of physical surveillances, motor vehicle and telephone toll record examinations, and interviews with informants, but it was the Title III surveillance which made the case.

My statement details, step-by-step, the manner by which a Title III surveillance is requested, approved, implemented and regulated. I think you will find that the rights of the citizen are well protected against unreasonable government action; and are provided a fair balancing against competing societal rights, both by the internal administrative procedures of the FBI and the Department of Justice, and an intervening magistrate.

THE CHRONOLOGY OF THE USE OF TITLE III ELECTRONIC SURVEILLANCE IN AN FBI CRIMINAL INVESTIGATION

A. Preliminary Investigation and Preparation of Affidavit

1. It is established through informant information or other general investigation, that a Federal criminal violation is being committed.

2. Further follow-up, corroborating investigation is conducted through contact with informants, physical surveillances, and general investigation.

3. An opinion of a Federal Strike Force Attorney or United States Attorney as to the prosecutive potential of the alleged violation is obtained.

4. An affidavit for application for a Title II electronic surveillance is prepared by the case agent after all other efforts to acquire necessary evidence have been exhausted.

5. The affidavit is reviewed by the legal officer in the FBI field office for probable cause and legal sufficiency and then submitted for review to a Strike Force Attorney or United States Attorney.

6. If the Strike Force Attorney or United States Attorney approves the affidavit, it is forwarded to FBI Headquarters.

B. Review of Affidavit at FBI Headquarters and Department of Justice

1. The affidavit is reviewed by the Office of Legal Counsel, case supervisor, his unit chief, section chief, Deputy Assistant Director, Assistant Director, Deputy Associate Director, Associate Director, and Director.

2. If the Director of the FBI approves the affidavit, it is forwarded to the Office of Special Operations, Department of Justice, for review, and it is submitted up the chain of command at the Department of Justice for final approval by the Assistant Attorney General, Criminal Division.

3. If the affidavit is approved by the Assistant Attorney General, it is sent back to the appropriate Strike Force Attorney or United States Attorney and FBI field office.

C. Application for Court Order

1. When the approved affidavit is received by the case agent, he files it before a United States District judge along with an application for the surveillance.

2. If the judge approves, he issues a court order directing the FBI to conduct the requested surveillance for a specified period of time which is set forth in the court order, usually 15-20 days.

3. This court order is then served upon the telephone company by the FBI agent to secure the necessary technical information and assistance to install the surveilance.

D. Operation by the FBI of a Title III Electronic Surveillance

1. After the necessary technical information and assistance is obtained, FBI personnel install the surveillance.

2. FBI supervisory personnel at the field level including the Special Agent in Charge, field supervisor, and case agent, inform all personnel who will participate in the surveillance of the investigation to be conducted. The legal officer also advises all personnel of legal limitations concerning monitoring, such as husband-wife, lawyer-client relationships.

3. A monitoring room is set up and specialists brief all participating personnel concerning the technical equipment and its operation.

4. Once operation is initiated, all surveillance activity is closely coordinated with operations within the monitoring room, i.e., limited to participating personnel and investigators with a need to know the results of the surveillance.

5. All results of the surveillance are recorded, i.e., pertinent tapes are transcribed and logs are maintained of all surveillances.

6. The Strike Force Attorney or United States Attorney is kept informed, on a daily basis, of the results of the surveillance.

7. The field office is required to inform FBI Headquarters every two days of the results of the surveillance.

8. The Strike Force Attorney or United States Attorney must inform the United States District Court which approved the surveillance of its results at intervals specified in the order.

9. Extensions or renewals of the surveillance are requested by the United States Attorney or Strike Force Attorney.

E. Termination of the Surveillance

1. At the termination of the surveillance, the tapes are sealed and are retained at a location specified by the District Court for a period of ten years. Pertinent information from the tapes, necessary for further investigation, is made available to investigators with a need to know.

2. Results of the surveillance are included in affidavits to support search and/or arrest warrants.

F. Prosecution

1. Evidence obtained during the entire investigation, including information developed through Title II interception, evidence seized in raids, and information developed through general investigation is presented to a Federal grand jury. If indictments are returned, arrests are made.

2. Upon motion of defense attorneys, a suppression hearing is generally held before a United States District Court judge at which probable cause, and the consequent legality, of all warrants, including the Title III warrant, are tested.

3. Prior to trial, the United States District Court orders relevant Title III tapes unsealed and the government to furnish copies of these tapes and transcripts to defense attorneys.

My statement also contains some examples of the value of consensual monitoring, i.e., monitoring of conversations with the consent of one party to the conversation. This technique is used significantly in organized crime cases, in which perjury intimidation or murder of witnesses, and destruction of evidence are not uncommon phenomena. A mechanical reproduction of a conversation and a law enforcement officer/witness who monitored the conversation have been indispensable to successful prosecution in several cases, and because there has been independent evidence of a conversation, the life of the party who consented to the monitoring who might otherwise have been the only witness, may have been saved.

As previously noted, consensual monitoring has assisted in not only solving kidnapings but may also have saved victims' lives.

CONSENSUAL MONITORING

In United States v. White, 401 U. S. 745 (1971) (regarding the use of a transmitting device concealed on the person of an informant) Justice White, speaking for the Court stated:

"Concededly a police agent who conceals his police connections may write down for official use his conversations with a defendant and testify concerning them, without a warrant authorizing his encounters with the defendant and without otherwise violating the latter's Fourth Amendment rights. . . . For constitutional purposes, no different result is required if the agent, instead of immediately reporting and transcribing his conversations with the defendant, either (1) simultaneously records them with electronic equipment which he is carrying on his person . . . (2) or carries radio equipment which simultaneously transmits the conversations either to recording equipment located elsewhere or to other agents monitoring the transmitting frequency. . . . If the conduct and revelations of an agent operating without electronic equipment do not invade the defendant's constitutionally justifiable expectations of privacy, neither does a simultaneous recording of the same conversations made by the agent or by others from transmissions received from the agent to whom the defendant is talking and whose trustworthiness the defendant necessarily risks.

". . . the law permits the frustration of actual expectations of privacy by permitting authorities to use testimony of those associates who for one reason or another have determined to turn to the police, as well as by authorizing the use of informants. . . . If the law gives no protection to the wrongdoer whose trusted accomplice is, or becomes a police agent, neither should it protect him when that same agent has recorded or transmitted the conversations which are later offered in evidence to prove the State's case."

FBI regulations require that either the Special Agent in Charge of a local field office or, in sensitive cases, FBI Headquarters must personally approve all consensual telephonic overhearings. Justice Department regulations require Departmental approval for all other consensual monitoring, i.e., concealed radio transmitters or recording equipment.

The value of consensual monitoring is evidenced by the following case:

Between 1968 and 1970 two Long Island businessmen had been paying off a usurious business loan to Joseph Randazzo and Giuseppe Maida. During this time the victims alleged that they had been subjected to threats of physical harm, at times involving guns, kickings, and beatings. In November, 1970, the victims made telephone calls to Vincent Lore, an associate of Randazzo and Maida, who had been involved in physical attacks on the victims. These calls were monitored by FBI agents and incriminating evidence was obtained. Justice Department authority was given to equip the victims with body recorders to monitor future conversations with Randazzo, Maida, and Lore. Based in part on evidence recorded, Randazzo, Maida, and Lore were arrested, and eventually pleaded guilty to extorionate credit transactions.

Hoodlum loan sharking, because of the violence often associated with it, is

one of the most vicious and profitable enterprises engaged in by the organized underworld. In this case, without the use of consensual monitoring devices, it is questionable whether successful prosecutions could have been obtained since murder of the businessmen could have eliminated the only witnesses to the criminal activity.

I have also included in my prepared statement a detailed analysis of the bills pending before this Subcommittee and the impact they could have on FBI operations.

H.R. 1597

H.R. 1597 requires that electronic surveillance of a United States Judge or Justice or a Senator or Member of Congress can be conducted only on the written authorization of the President of the United States.

The FBI has no comment on this bill; it in no way affects FBI operations.

H.R. 9667 (ALSO INTRODUCED AS H.R. 9973, H.R. 10008, AND H.R. 1033) H.R. 9698; H.R. 9781

Via different types of amendments to 18 U.S.C. 2511, these bills either totally prohibit electronic surveillance of any type, for any reason (H.R. 9781), or require the consent of all parties to the conversation to be monitored except when a judicial warrant has been issued. (H.R. 9667, H.R. 9698).

The FBI is opposed to H.R. 9781; and constitutional problems may be presented by H.R. 9667 and H.R. 9698.

Electronic surveillance is an effective, and often a unique investigative technique by which information essential to a successful prosecution or thwarting of foreign intelligence or terroist activity is obtained which is not available from any other source. Electronic surveillance is an essential investigative tool in combating organized crime; it has been used effectively, fairly, and without prejudice to individual rights in bribery, embezzlement, Hobbs Act, obstruction of justice, interstate theft, kidnaping extortion, sports bribery, and racketeering cases.

Congress has weighed the need for electronic surveillances in these, and other types of cases; and, finding that the need was real and necessary, provided a mechanism and authority for the fair and effective use of electronic surveillance, while protecting the individual in his right to due process and against unreasonable search and seizure—Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

Use of electronic surveillance in these cases has been of utmost value to fair and efficient law enforcement. As the Subcommittee is aware, use of Title III during the six years since its passage will undergo a year-long examination by a committee of experts appointed by the Congress. The committee begins its study this year. I am confident that the committee's report will support my general observations that Title III has provided law enforcement with an effective and indispensable investigative tool, and its use has been administered fairly, without prejudice to individual rights.

These bills would prohibit even the listening in to a telephone conversation by a law enforcement officer at the request of a party who was being extorted or was receiving ransom instructions via the telephone. This practice is often instrumental in the return of the kidnaped victim safely, and in the solution of the crime.

It should not be assumed however that a Title III warrant could be obtained in all, or even in many, of these types of cases. An allegation of organized crime loan sharking originally consists of just the word of the victim, plus some general knowledge of the subject's background. This is generally not sufficient to support a Title III application, but at the time the victim comes to us he is generally already in some danger and there is no time for extensive general investigation to support an affidavit, hence we use a consensual monitoring device to obtain the necessary incriminating evidence rapidly.

In kidnaping cases the call to the victim's relatives often occurs within hours after the kidnaping; there is no time to run a Title III application through FBI and Department of Justice administrative channels to obtain the Attorney's General prior approval, required by Title III, much less present the application to a court.

H.R. 9815 (ALSO INTRODUCED AS H.R. 11629)

The heart of H.R. 9815 is a prohibition against any civil officer of the United States or officer of the United States Armed Forces from employing any part of the United States Armed Forces or any State militia "to conduct investigations and to maintain surveillances over, or record or maintain information regarding, the beliefs, associations, or political activities" of non-Armed Forces personnel or members of any civilian organization.

I assure the Subcommittee that the FBI does not utilize military personnel in its domestic internal security investigations.

However, H.R. 9815 presents serious difficulties for our current practices, and our continuing investigative needs, in the foreign counterintelligence area. This is a matter which must be reserved for executive session.

H.R. 9949

H.R. 9949 seeks to amend 18 U.S.C. 2511(3) by adding the following sentence:

"Nothing contained in this paragraph shall be deemed to authorize the President, or anyone acting or purporting to act on his behalf to engage in burglary or any other illegal act that is not prohibited by this chapter."

Section 2 provides that nothing previously enacted or hereafter to be enacted by Congress shall authorize the President to engage in burglary or any other illegal act without express statutory authorization of Congress.

H.R. 9949 merely bolsters the interpretation that 18 U.S.C. 2511(3) was merely Congress's disclaimer that Title III of the Omnibus Crime Control and Safe Streets Act of 1968 did not in any way affect constitutional Presidential powers.

The bill neither adds to nor detracts from constitutional Presidential powers to conduct foreign affairs; to preserve, protect, and defend the Constitution; and to protect the States against invasion.

H.R. 9949 seeks merely to make it clear that 18 U.S.C. 2511(3) cannot be cited as any type of congressional *authority* for Presidential action.

As such, the FBI has no comment on the bill, since it does not affect current FBI operations. However, while the FBI also interprets 18 U.S.C. 2511(3) as congressional disclaimer of any intent to affect, i.e., to expand, restrict or define Presidential powers, we do, when requesting approval from the Attorney General for foreign counterintelligence electronic surveillances, cite the areas of Presidential powers enumerated in 18 U.S.C. 2511(3) as an indication that Congress, and the people, do feel there are constitutional Presidential powers in these general areas.

H.R. 11838

H.R. 11838 seeks to amend 18 U.S.C. 2516(1) and (2) by eliminating the provision for an "emergency" electronic surveillance permitted under 18 U.S.C. 2518(7). 18 U.S.C. 2518(7) permits an electronic surveillance to be installed without prior court approval in an emergency situation, provided that court approval is subsequently obtained within 48 hours.

H.R. 11838 avoids the tack of attempting to repeal 18 U.S.C. 2518(7) by amending 18 U.S.C. 2516(1) and (2) so that these subsections can only be read as requiring *prior* judicial approval of electronic surveillances in all cases.

As an indication of the discretion with which the FBI utilizes Title III electronic surveillances, I point out that the FBI has never used the emergency provision of Section 2518(7); however, this is merely to emphasize that we recognize the sensitivity of such a provision, and to refute the notion that if Congress gives the Executive an exception it will make the exception the rule.

Although we have never used the emergency provision, I resist its revocation. Congress has recognized that in unique serious situations in which urgency does not allow for the pre-surveillance warrant procedure the Executive should have the means to utilize a surveillance.

If restrictions on consensual monitoring are effected, I can foresee where we would be forced to utilize the emergency provision in many kidnaping, extortion, and perhaps organized crime cases.

H.R. 13825

H.R. 13825 presents both constitutional and practical problems. In general, the constitutional problem presented is that the bill would have Congress define and regulate powers and actions of the President in areas which have heretofore been referred to as constitutional. The question is then whether these powers are, in fact, constitutional, and if so, Congress would apparently have no authority to legislate in those areas.

The practical problems presented apparently stem from a lack of understanding of how foreign intelligence services operate in the United States; how electronic surveillance is utilized in this area; and how use of the technique is now controlled.

The bill specifically tells the President whom he may subject to electronic surveillance in taking actions he deems necessary to protect the Nation against hostile acts of a foreign power, or to obtain essential foreign intelligence information, or to protect national security information against foreign intelligence activities. Under the bill, the President may only employ electronic surveillance against "foreign agents," whom the bill defines as ". . . any person who is not an American citizen or in the process of becoming an American citizen and whose first allegiance is to a foreign power and whose activities are intended to serve the interest of that foreign power and to undermine the security of the United States."

The bill tells the President how he is to implement an electronic surveillance against a "foreign agent" by referring him to a new provision of Section 2518A which embodies a lesser standard of proof than "probable cause to believe a crime has been or is about to be committed."

The bill deletes that provision of Section 2511(3) which exempted from Title III of the Omnibus Crime Control and Safe Streets Act of 1968 those actions as regards electronic surveillance taken by the President ". . . to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government." This deletion, in essence, forces the President into the current provisions of Title III as regards electronic surveillance in all national security cases involving United States citizens.

The bill amends Section 2511(3) to prohibit the contents of any communication of a "foreign agent" intercepted pursuant to a warrant issued in accordance with Section 2518A from being used as evidence in a court proceeding, except civil proceedings against "foreign agents." Although the legislative policy behind the "civil proceedings" clause of this provision is obscure, the evident purpose of this section is to insure that no individual, whether a "foreign agent" or not, is deprived of his liberty on the basis of information obtained during an interception of communications in a case wherein the lesser standards of probable cause of 18 U.S.C. 2518A had been employed to secure the warrant.

Recently, the Supreme Court, in United States v. United States District Court (407 U.S. 297 (1972), commonly referred to as the *Keith* case, noting that Congress specifically disclaimed any effect on the constitutional powers of the President in Title III, observed that Congress might wish to prescribe protective standards for domestic security surveillances which would differ from standards already prescribed for Title III criminal surveillances. The court commented that different standards for the two kinds of surveillances "may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."

H.R. 13825 evades the difficult questions presented by the distinctive character of intelligence investigations in the determination of the "balance-point" at which certain intrusions into privacy incident to intelligence collection are outweighed by the public benefits to be gained. The bill does this by transposing the "probable cause" standard of the Fourth Amendment as it pertains to the commission of a crime into the field of pre-crime, intelligence investigation as it relates to electronic surveillance of United States citizens.

It appears that H.R. 13825's wholesale transposition of Fourth Amendment criminal law standards pertaining to "probable cause" negatively affects the authority of the President to meet a foreign intelligence threat in at least two ways: (1) It has forced the adoption of an impractical definition of

"foreign agent." This result has occurred because transposition of Fourth Amendment standards requires that the bill define those individuals whom the President has power to defend the Nation against as being non-United States citizens in every instance. In many cases, agents of foreign intelligence services are American citizens. (2) By excluding from trial all evidence obtained from an electronic surveillanec unless obtained under a warrant based on probable cause that a crime had been or was about to be committed, H.R. 13825 would probably preclude use of information obtained from an intercept conducted with a judicial warrant, under the Section 2511(3) constitutional presidential powers provision, in the prosecution of a foreign intelligence officer who did not possess diplomatic immunity. In many cases electronic surveillance of known intelligence officers is conducted without probable cause, in the traditional criminal law understanding of that term, but it eventually produces evidence of intelligence gathering in violation of criminal laws.

Section 2518A(2) requires that application for a court order authorizing an intercept against either a "foreign agent" (under Section 2511(3)) or a United States citizen (under Section 2516A) must furnish "evidence" that the intercept shall serve one of the purposes of these two sections. In the foreign counterintelligence field this requirement presnts significant difficulties. Discussion in this area has to be reserved for executive session.

Subsection 2518A(8) provides that anyone whose communications are intercepted pursuant to Section 2516A be furnished copies of the affidavits, the order, and relevant transcripts within thirty days. Although this provision excepts intercepts against "foreign agents" under subsection 2511(3) its value is nullified by the requirement that the intercept would have to be disclosed to anyone intercepted in communication with the targeted "foreign agent."

Prior to considering specific restraints, or conversely, grants of additional authority whether pertaining to interceptions of communications or other investigative techniques, it appears necessary for Congress to first give full and careful consideration to what it desires the FBI's function to be, particularly in the intelligence area. Only in this manner can we resolve the inconsistency between what the FBI views as its legitimate and mandated objectives, and the limitations being considered on our practices to attain those objectives.

Mr. KASTENMEIER. You are correct in stating that the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance will begin operations shortly. Our first meeting, and I am a member of that Commission, will be May 9. But, as so often happens with regard to subjects of national concern, the exigency of the situation tends to outrun the time required for the Commission's study. For example, the National Commission on Pornography and Obscenity was still deliberating when this subcommittee was called upon to consider legislation. We did not have the benefit of its final work product.

In any event, whatever legislative activity is undertaken by the Congress, in the field of wiretapping, the work of the Commission will be beneficial, and many of us have high hopes for it.

Has compliance with title III, posed any extraordinary difficulties for the Bureau since 1968?

Mr. MILLER. After the legislation was passed, we had studied the procedures, we felt—and I think Mr. Cleveland will support this—we felt that it was necessary for us to conduct extremely tight-knit, detailed investigations to develop sufficient probable cause to support a title III application. We felt that our probable cause statement and our applications for title III surveillances had to be highly detailed. We approached the problem with all sincerity, because we knew that we were in a sensitive area. We recognized the title III surveillance immediately as an extremely valuable tool for law

enforcement, and that resulted in an initial conservative approach on our part, and also on the part of the Department, which I think has stood us in extremely good stead. The probable cause statements in our applications have been extremely detailed.

Almost without exception the title III investigative technique has been highly valuable. Without it we most certainly could not have compiled the record that we have compiled in the organized crime area. We look at title III as a very fine piece of legislation.

Mr. KASTENMEIER. On page 2 of your statement you indicate your concern with abuses of electronic surveillance, and you suggest that these abuses are a detriment to its fair, legitimate, and effective use as a tool. What abuses did you have in mind, Miller?

Mr. MILLER. Some of the abuses perhaps are real. Some of them are, I am sure, imagined.

Mr. KASTENMEIER. Whether or not they are real, abuses have been reported.

Mr. MILLER. Yes. I think that the entire wiretapping controversy has been much overplayed. By that I mean the abuses that are alleged, perhaps because of the nature of the investigative technique, have gotten a tremendous amount of publicity. One of the abuses that I can think of that has been alleged was in the Wounded Knee prosecution out in St. Paul. That situation involved a nine-party telephone line—it was simply a party line—which had been cut, but was reinstalled and paid for by the Government, in order to maintain communication with the occupiers and facilitate negotiation. The Government became a party to this line by having a phone installed at Road Block One. That extension that the Government had has been alleged to have been a wiretap.

Now, we do not look at that as a wiretap. To us it was merely an extension.

Another instance where wiretap abuse was alleged, was down in Gainesville during the so-called "Gainesville Eight" trial. That was an unfortunate fortuitous situation. We routinely sweep our resident agencies and our field offices for electronic surveillances directed against us. The schedule for the sweep of the resident agency in Gainesville, Fla., coincided with the beginning of the 'Gainesville Eight" trial. The fact that the trial had begun that day was unknown to the men who were conducting the sweep of our office space down there. They had also been requested to conduct a sweep of the U.S. Attorney's office and the marshal's office in the same Federal building. The two men who were conducting this sweep, which occurred somewhere in the vicinity of 5:30 or so in the evening, were in a wire closet looking over the pairs in the closet, and unknown to them, in the very next room the defense counsel had been given space in the Federal building. The defense counsel, and I believe some of the defendants, were in this room and heard conversations in the room next to them, which was the wire closet. This became quite a topic of conversation. It was reported immediately to the trial judge who held that same evening very detailed hearings in which the defendents and our agents testified under oath. The telephone company was requested to bring in experts, and they went over the entire vicinity immediately to determine

whether or not this was a wiretap effort on the part of the FBI. It was not. We would have preferred not to have had it happen because it was embarrassing to us. Whether or not it had any effect on the results of the trial, we do not know. But, as I say, we would prefer—would have preferred—that this not happen. But, it did.

The situation itself was thoroughly looked into by the judge and resolved completely; in his opinion, it was not a wiretap effort on the part of the FBI. And, indeed, it was not. But, you see what I mean, it has been alleged that both these instances involved wiretap abuses.

Mr. KASTENMEIER. On the question of responsibility, are all domestic wiretaps, whether or not pursuant to a warrant, cleared or processed by the Department of Justice in general, and the Bureau, in particular?

Mr. MILLER. In the FBI, from an investigation standpoint, we have responsibilities in three principal areas. The first area is criminal. In this area we use title III wiretaps.

The second area is counterintelligence; which, in its entirety, involves foreign intelligence.

Now, in these two areas, we can and do use wiretaps.

In the third area, which is domestic intelligence, we do not have any mechanism for using wiretaps, and we have not conducted wiretaps since the *Keith* decision on June 19, 1972. And that is the area in which we say that we should discuss with Congress some measures to provide for wiretap procedures. If we had a wiretap capability in a situation like the Symbionese Liberation Army case in California, a domestic intelligence case, we feel that we could perhaps thwart some of the further complications that grow out of such cases; for example, where the espoused revolutionary purposes people engage in what they call urban guerilla warfare, expropriations and things like that. We feel that in that area, *Keith* has created a definite void.

Mr. KASTENMEIER. Yes.

Mr. SMITH. Mr. Chairman, could I interrupt right at that point?

Mr. KASTENMEIER. Yes. The gentleman from New York.

Mr. SMITH. Well, Mr. Miller, in that type of case, why can't you now use title III surveillance pursuant to court order?

Mr. MILLER. We have studied this problem very carefully, and did right from the outset on June 20 of 1972, whenever this——

Mr. SMITH. Was this right after the *Keith* case?

Mr. MILLER. Right after the *Keith* case, yes, sir.

We studied that particular situation very carefully at that time, and have continued to do so since. There are two principal problems. The first problem is with the development of sufficient probable cause required by the omnibus crime bill of 1968. To develop that kind of probable cause is, in an intelligence-gathering effort, virtually impossible. The second problem for the FBI when conducting an open-ended intelligence-gathering effort, is that notice of surveillance would have to be divulged at the termination of 30 days or whatever. That is the thing that makes the use of title III impractical in an ongoing intelligence investigation. We have not been

able to satisfy either of these two requirements in domestic intelligence cases.

Mr. COHEN. Would the gentleman yield for a question?

Mr. SMITH. I will be happy to yield.

Mr. COHEN. If I could follow up on that, you say it is virtually impossible to gather intelligence under title III for this purpose. How many attempts have you made to present a warrant to a court for such a wiretap, and how many have been rejected? Could you tell us?

Mr. MILLER. In this particular area, Mr. Cohen?

Mr. COHEN. Yes.

Mr. MILLER. We have not yet been able to satisfy either ourselves or the Department that we have had enough probable cause, as traditionally understood on which to base an application.

Mr. COHEN. If you do not have enough evidence for probable cause, then wouldn't that seem to negate the basis for a wiretap in the first place?

Mr. MILLER. I missed part of your question.

Mr. COHEN. If you do not have enough evidence in these cases to establish probable cause, without a warrant, then why are you seeking it in the first case? I mean, if there is not enough there to get a warrant, it seems to me you should not be allowed to conduct a warrantless wiretap.

Mr. MILLER. Well, we have not been able to do that, as I say.

Now, the kind of investigation that we are talking about is an intelligence-gathering situation. For example, and here again we can go into this SLA situation, we would like very much to have long since obtained sufficient intelligence information to resolve that problem out there from an investigative standpoint. From an intelligence-gathering position, we feel that there may have been places where a domestic intelligence electronic surveillance would have been productive in helping to solve the actual kidnaping and extortion case itself; however, it is extremely difficult in such a case to develop the kind of probable cause that is necessary for a regular title III surveillance. To clarify, we are not talking about the actual place that these few SLA members were holding the victim; we do not know that. We are not talking about their telephone. We are talking about somebody else's telephone who might be in logistical or tactical support of the kidnaping and extortion effort. Developing that kind of probable cause on this second party is extremely difficult. Yet, from an intelligence standpoint it could, and would, possibly have been extremely productive in solving this case.

Mr. COHEN. I do not want to use up any more of the time.

Mr. KASTENMEIER. Just to follow up on the gentleman from New York's question, you said you had two problems. The first is that it is difficult to develop sufficient probable cause. What is the second problem?

Mr. MILLER. The second problem is in divulging to the person tapped, in an ongoing intelligence, gathering situation within the requirements of title III. That represents a problem also, because these are, in most instances, open-ended intelligence-type kinds of investigations.

Mr. KASTENMEIER. One of the questions I wanted to go back to concerns the three classes of potential uses for electronic surveillance or wiretapping. In particular, I am interested in the distinction between the second and third classes, the counterintelligence or foreign intelligence and domestic intelligence. I am wondering what your definition of each of these two classes of intelligence is?

Mr. MILLER. These are really two different areas that we're talking about, but they do overlap in trade terms. In other words, when you use the term internal security, that could include both categories, both purely domestic intelligence-gathering efforts and also counterintelligence. We like to break them down in order to keep our own minds clear.

Counterintelligence efforts on our part, and that is Mr. Decker's branch in the Intelligence Division, deal primarily with just what that says, countering foreign intelligence services. Some foreign countries undertake intelligence-collection efforts operating inside our country. Mr. Decker's work is to counter their intelligence efforts.

In the domestic area we are talking primarily about people who are U.S. citizens or residents—people who are espousing revolution, people who are talking about violence, people who are talking about terrorism, including bombings. Some of these people have borrowed philosophies and tactics from other countries, but their activity is essentially domestic.

Mr. KASTENMEIER. Would an American citizen alleged to be an agent of a foreign power operating in this country, fall within your second category while such a citizen, not associated with a foreign power, fall within your third category?

Mr. MILLER. Yes, sir. That is primarily it; although domestic threats may be philosophically associated with a hostile foreign power.

Mr. KASTENMEIER. But there is no allegation that they take direction from this foreign power?

Mr. MILLER. No, sir.

Mr. KASTENMEIER. Or are agents per se?

Mr. MILLER. No, sir. That is right. And as far as nationality in the foreign area is concerned the key word there is not whether an individual is a citizen or not. A foreign power could, if we built a wall around that word "citizen," have their people become citizens, and then operate with immunity. We look at what the individual is doing rather than at his citizenship; that is, is this man a spy; is this man a saboteur, an espionage agent, and so forth. If he happened to be a citizen, most certainly that would be weighed very carefully by us and the Department in discussing authorization for a wiretap. But, the real issue would be, even though this fellow is a citizen, is he a threat to this country because he is an espionage agent?

Mr. KASTENMEIER. Returning now to my earlier question. You were analyzing the three categories of national security surveillance, and I was asking you what role the Bureau played in conducting domestic activity wiretapping and electronic surveillance. Would any national security surveillance need to be cleared through the Department of Justice, specifically through the Bureau, if conducted within the continental United States?

Mr. MILLER. Oh, yes. Most certainly.

Mr. KASTENMEIER. In other words, it does not matter whether it is the Internal Revenue Service or the Department of Defense, the tap would be, in the final analysis, accounted for by the Bureau?

Mr. MILLER. The answer to that question is yes. If it is a national security wiretap situation in the United States, then the FBI would be the one to handle it.

Mr. KASTENMEIER. Do applications come from a source external to the FBI, the Bureau, or the Justice Department? Sometimes the FBI, it would appear, might have to take the blame, but they were not the ones who requested the tap? For example, I do not know in the Wounded Knee situation whether the Department of the Interior or some other department might have requested it. Not all requests for wiretap applications originate with the Bureau, I take it. Is that correct?

Mr. MILLER. We considered a title III wiretap in the Wounded Knee situation; however, the actual application was never perfected to the point where it was approved.

Now, we handle only our own title III situations. And if we do get them approved, then we handle the entire operation.

However, in the criminal field, Federal investigative agencies which can obtain title III surveillances and they handle their own requests through the Attorney General. And if they are approved, then they handle them themselves. We do not handle the mechanics or the collection of title III information for other Federal investigative agencies.

Mr. KASTENMEIER. For example, the Secret Service or some similar entity would go to the Attorney General, but the Bureau would not be called on to handle it?

Mr. MILLER. We would not even know it. Yes, sir. The narcotics people, for example, if they had a title III situation, they would submit their application to the Department. And if it were approved, and subsequently approved by a judge, then they would handle the entire thing and we would not be knowledgeable of that whatsoever.

But, in the national security area, Mr. Johnson, in 1965, I believe it was, by Presidential directive, said that all national security electronic surveillances would be approved by the Attorney General, and the Attorney General has directed that we will handle them. So, in those instances, as distinguished from title III, we would handle the entire situation—the application for, the technical handling of, and the furnishing of the product back to whomever requested it.

Mr. KASTENMEIER. What departments would make that request of the Attorney General and of you in the national security area?

Mr. MILLER. In the national security area there are three departments which may do so. One is the Central Intelligence Agency, another is the State Department, and the other is the National Security Agency.

Mr. KASTENMEIER. The Defense Department does not have the authority to make such an application to you?

Mr. MILLER. We have—to my knowledge—never handled that kind of a situation for the Defense Department.

Mr. KASTENMEIER. I have only one other question before I yield. I have some questions in another area which I can reach later after my colleagues have had an opportunity to present questions.

Does the Bureau have any responsibility for wiretapping and electronic surveillance outside the United States?

Mr. MILLER. No, sir, none whatsoever.

Mr. KASTENMEIER. Presumably Government agencies which, on behalf of the United States, do conduct wiretapping and electronic surveillance abroad, maintain their own records in connection with such practices?

Mr. MILLER. I would presume so. I have little or no knowledge regarding that kind of a situation.

Mr. KASTENMEIER. In the area of foreign intelligence gathering, I assume those agencies gathering such intelligence would probably have their own system of accounting?

However, the Bureau has agents abroad? Do you have a separate accounting for the activities of these agents?

Mr. MILLER. We do have agents abroad. We call them legal attachés. They function only in a liaison capacity with police agencies in whatever foreign country it would be. In London, for example, our men deal very closely with Scotland Yard. There is an exchange, what we call foreign police cooperation.

We have no capability whatever in the wiretap area outside of the United States.

Mr. KASTENMEIER. I was thinking of a case where an Embassy, for example, in London, might have reason to believe that some of our own people should be checked. Would they not go to the Bureau or your officer within the Embassy for help in wiretapping or conducting electronic surveillance with respect to such people?

Mr. MILLER. No. They may discuss it with them.

Mr. KASTENMEIER. They would have to have their own people?

Mr. MILLER. Our legal attaches are very qualified people, and in the situation you describe, Embassy personnel may well discuss it with the agent who is there in that capacity; however, he would not perform that kind of a service.In each of the Embassies they have a person who is in charge of the security of the Embassy, and wiretapping would get into a security type——

Mr. KASTENMEIER. And that would be within the Department of State in that case?

Mr. MILLER. Yes. Part of the State Department Security Office.

Mr. KASTENMEIER. At this time I would like to yield again to the gentleman from New York, Mr. Smith.

Mr. SMITH. Mr. Miller, does the FBI have any procedure for assuring the privacy of those whose conversations have been intercepted? For example, are records of conversations intercepted that have nothing to do with what you are interested in destroyed at some time? Is there any provision for protecting the privacy of those conversations?

Mr. MILLER. In answer to your first question, Mr. Smith, no the records are not destroyed. The records are kept; however, provisions for protecting individual privacy are quite detailed.

For example, if an individual is discussing a matter with his attorney, and the person monitoring the conversation recognizes this, either at the outset from the name of the individual, or from his own experience, then he does not monitor that conversation. Now, if it happens accidentally, then our instructions are that this be called to the attention of the U.S. attorney immediately, and the conversation—tape and log—are sealed so that there is no attorney-client conversation available to the prosecution. But, it is not destroyed.

In the normal routine of monitoring these wiretaps, as you say, there are extraneous conversations intercepted. They are recorded and logged, but not all of them are indexed. If you index it, then you have the capabiilty of going back and finding it. Much information is not indexed. It is, when it is thought to be pertinent to the investigation being conducted. We maintain what we call our electronic surveillance indices, so that in a subsequent proceeding, or whenever the Department is trying to make a prosecutive determination, we can determine if a man has ever been overheard. He may not be the subject of the wiretap, but the Department wants to know if he has ever been overheard. And we check our records to see if he has been overheard, and if he has we furnish the information to the Department. All of this goes into the determination of whether to prosecute or not.

Now, let us say an individual has been indicted, trial has been set, and pretrail motions are being heard. The attorney and the defendant come to the court, and in their pretrial motions one of the questions which has come to use in most instances is have I, the defendant, or my attorneys, or their associates ever been overheard on an electronic surveillance—the scope of this inquiry has been extended quite broadly. Then we can check the records of the entire FBI, not only headquarters but every pertinent field office, to respond to this request from the defendant and to make sure that we give him as perfect a product as possible.

Now, in national security cases electronic surveillance results are reviewed in camera by the judge sitting in the case. He reviews the material to determine if it is pertinent to the trial, and whether the Government's case is tainted by an illegal electronic surveillance. That determination is usually made by the judge who is sitting in the case before the trial ever begins, and sometimes the judge does determine that the material, in its entirety, should b given to the defendant. Sometimes he determines that it is not pertinent, has not tainted the Government's case, or has not been a lead to further the investigation, in which case he does not direct that the material be given to the defendant.

Mr. SMITH. Thank you, very much.

Mr. MILLER. Yes, sir.

Mr. KASTENMEIER. The gentleman from Massachusetts, Mr. Drinan.

Mr. DRINAN. Thank you very much, Mr. Chairman.

Mr. Miller, I read your testimony over the weekend with the greatest care, and when I read on page 3 that "I support measures to carefully regulate and control the use of wiretapping" my heart

leapt up. But, I do not find any measures that you support. You say that you hope in the near future to present to Congress a bill. But, in the whole latter part of your testimony you shoot down every bill that has been proposed to fill the void which you admit has existed for 2 years since the *Keith* decision. You mention abuses, but when the chairman cross-examined you I didn't hear about abuses. But, I would like to ask you about the origin or the sources of these abuses so that I can get your philosophy on this matter.

Let us take the Dr. Kissinger taps, for example, the taps of 13 Government employees and four newsmen. What I want to find out is, what you think could be an abuse? Is it an abuse when the National Security Council tells the FBI to put a wiretap on these 17 people, and the FBI complies with the request? Four newsmen and 13 Government employees, including Morton Halperin, were wiretapped. And Dr. Halperin's wiretap was for 21 months, only four of which he was a Government employee. Were these abuses?

Mr. MILLER. I do not think so, Mr. Drinan. That, of course is a unique situation, unique to the FBI.

Mr. DRINAN. There were no abuses. What could be an abuse? You admit that abuses have occurred and that you want to help us to correct these abuses, but you have not helped me at all, I am sorry to say, because I do not know what would be an abuse according to your philosophy.

Mr. MILLER. I would say that an abuse, in my philisophy, would be somebody who wiretapped an individual without having gone through the authorization procedures.

Mr. DRINAN. That is not an abuse. That is lawlessness, sir. I want to talk about the inadequacies and limitations in title III, and the bills that are proposed by people like Senator Gaylord Nelson, and by the chairman, and by others to remedy what they conceive to be abuses. What do you conceive to be abuses in the present and existing systems?

Mr. MILLER. Abuses in the present system would be the types of situations that you term lawlessness. Now, in getting back to the other question on the special coverage. I want to say that we have furnished information to the Special Prosecutor on that issue and also we are in the process of furnishing information to the House Judiciary Committee on the same issue. We are furnishing all of the information that we have.

Mr. DRINAN. But you have already said there was no abuse in the whole Kissinger wiretap situation.

Mr. MILLER. Well, in getting back to that——

Mr. DRINAN. Do you want to qualify your answer?

Mr. MILLER. Well, I do not term it an abuse. Based on the thinking that prevailed back at that time in 1969, whenever this technique was employed, the Government had what I feel was a very serious problem.

Mr. DRINAN. Yes. I am familiar with that, sir. It is set forth in the brief in Dr. Halperin's case. I have no idea what kind of legislation you might propose. You say we hope in the near future to present to Congress a bill, but what would that bill be?

Mr. MILLER. That would be primarily, as I indicated here in the area of domestic intelligence collection, to see if there is some way for the FBI, some way to put a magistrate, a judge, or somebody, between the FBI and an assassin, or a terrorist, or a kidnaper, who is engaged in domestic, political, or urban guerilla warfare activities. Those are the things that I am talking about here, and the area where we see a void.

Mr. KASTENMEIER. Would the gentleman yield?

Mr. DRINAN. Yes.

Mr. KASTENMEIER. I really do not see how you make a distinction between that type of case, Mr. Miller, and organized crime which is being tapped extensively, and perhaps for every good reason. How are these terrorists, the would-be assassins that you mentioned, different from organized crime? Why couldn't you, under title III, get a tap authorized on groups such as the SLA?

Mr. MILLER. The main problem is divulging the wiretap to the individual whom you have tapped, or other individuals after some designated period of time. That is extremely hard to live with. In fact, it is impossible because these are open-ended intelligence gathering situations. Now, what we are talking about——

Mr. KASTENMEIER. Yes. Why would they be different than organized crime? You have the same problem with respect to members of organized crime, who are probably better equipped to deal with you in that context than these political revolutionaries who may be about to commit a crime.

Mr. MILLER. In organized crime areas, at the time that we develop the information for the application for title III, the crime is an ongoing crime, for example, a gambling crime. It is being committed today, tomorrow, the next day and so forth. Now, in the politically motivated crime areas, you are talking about things that are much more abstract. Individuals are talking about revolution, they are talking about developing plans for an assassination, they are talking about killing policemen, things like that. The crime, to our knowledge, is not being committed at that time. But, the plans are being made to commit it. We do not know when the crime is going to be committed. You really do not have a crime actually being committed at the time. You have the propensity for the crime and you have got the people talking about it.

For example, at one time in the SLA case, there may have been discussions concerning kidnaping, and the other things that were done. We feel that there was a point in that case where it would have been compatible with the best interests of the people of the United States to consider a wiretap to find out just what was being planned. The crime had not yet been committed. It was purely an intelligence gathering situation.

This, incidentally, is not an easy determination. We do not really see it as an easy problem to draw up a proposal for legislation in this area. We have serious problems with it ourselves.

Mr. KASTENMEIER. I understand your difficulty. However, as a citizen, I am not worried that you may have to divulge the existence of a wiretap to these people. I think maybe you ought to be doing it under title III even though, as you say, you do not like to divulge

things. But, you have had to do that with organized crime, and if they can cope with it as well as they have, or if you can cope with them as well as you have, I have a feeling that it would not be much different in this situation that you talk about now.

I yield back to the gentleman from Massachusetts.

Mr. DRINAN. Thank you. I gather, Mr. Miller, that the legislation that you are at least thinking about is not to correct abuses, but to get more power so you can have wiretaps for intelligence gathering with or without what is traditionally known as probable cause.

On page 11 you indicate that at least under title III, the court order is served upon the telephone company by the FBI to secure the necessary technical information and assistance to install the surveillance. A high official at the AT&T last Friday testified that there are roughly 100 wiretaps, without a warrant, that are acknowledged by the Department of Justice, but that far fewer wiretaps have come to the attention of the telephone company. Does the FBI sometimes tap phones without the knowledge or consent of the telephone company?

Mr. MILLER. I am trying to give you the best I can from my recollection. My answer is no, that on——

Mr. DRINAN. Are you disputing this high official whose testimony is on the record?

Mr. MILLER. Well, I have not read his testimony, Mr. Drinan.

Mr. DRINAN. His testimony was exactly as I said it, that Mr. Peterson said roughly there were 100 warrantless wiretaps in the last calendar year, and the AT&T throughout all of its affiliates has knowledge of far fewer than 100. And he draws the inevitable conclusion that the FBI or the Department of Justice or both are installing taps on telephones without the knowledge or consent of anybody in the AT&T. You do not have to see the testimony. What is your answer?

Mr. MILLER. All right. Well, in the first place, the AT&T would not necessarily be aware of the wiretaps, know about all of the wiretap situations, if another telephone company were involved.

Mr. DRINAN. I meant all of the affiliates of the Bell System, and he has told us that they have a record of far fewer than 100. He did not name the exact number. But, he indicated that it was substantially less than 100, and he himself drew the inference that the FBI obviously must be tapping telephones without telling anybody in the Bell System. And you said no, that you do not do it, right?

Mr. MILLER. Yes. His conclusion is incorrect.

Mr. DRINAN. What is the explanation of the discrepancy in the numbers?

Mr. MILLER. The discrepancy—the best I could do from an explanation standpoint, No. 1, we do not tap telephones without full authorization. We run these authorizations through the phone companies because they do the work for us. From an explanation standpoint, I would say that some of these wiretap situations have been in existence for a considerable period of time, primarily in the foreign field and written notification to the phone company has not always been a practice. That is of fairly recent vintage.

Mr. DRINAN. When did you start the new practice, Mr. Miller, of informing the telephone company? When did you stop tapping phones without the permission of the telephone company? You have admitted that you have changed the practice recently. When did you change the practice?

Mr. MILLER. No. I did not say that we changed the practice of informing the telephone company; however, the phone companies have not always required written notice—which is what the A.T. & T. representatives must be talking about.

Mr. DECKER. Different phone companies have different policies, and I mean different companies within the Bell System; some require what we refer to as a lease line letter in which we ask for their assistance in proceeding on a line at the usual commercial rates. Now, your question seemed to presuppose that whatever installations we have on were put on in the last year, and the phone companies were not aware of the 100 that you referred to in the past year. Well, some of these go back over an extensive period of time and I think that might resolve the problem you have as to numbers.

Mr. DRINAN. Would you answer the question that I asked of Mr. Miller, how many are out there without the knowledge of the telephone company?

Mr. MILLER. None.

Mr. DECKER. I do not know of any.

Mr. MILLER. There are none out there without the knowledge of some phone company.

Mr. DECKER. If the phone company is assuming that whatever we have on we put on in the last year, and they cannot come up with the 100 that you referred to during the past year, it would be because some go back over an extensive period of time.

Mr. DRINAN. If the telephone company were not legally required to do this, if they refuse to cooperate, what would the FBI do? It is under serious consideration by the A.T. & T.

Mr. MILLER. I do not know what we would do, Mr. Drinan, at this point. We would most certainly want to discuss the matter.

Mr. DRINAN. Suppose the Congress made a law that the A.T. & T. may not allow the telephone wires of its subscribers to be tapped?

Mr. MILLER. I do not know what we would do. We would have to discuss that. Most certainly we would want to discuss the problem in view of the very important foreign policy and counterintelligence matters involved. We would want to discuss those problems with the Congress, not for the good of the FBI, and please do not misunderstand me. The FBI is not—we are not doing any of this work only for the good of the FBI.

Mr. DRINAN. No. I didn't mean that, sir. I understand that.

But, on another point, on page 17, you talk of the euphemism about consensual monitoring, and I am afraid that in my judgment that is a misleading term. It really means that there is a certain form of deception and entrapment involved. You say on page 17 that FBI officials in the local field office, special agents in charge, have to give permission, and in sensitive cases, they have to go to the FBI headquarters. Is there any record of such permission being denied for what you call euphemistically consensual monitoring?

Mr. MILLER. Those procedures concerning consensual monitoring deal with the telephone itself.

Mr. DRINAN. What?

Mr. MILLER. The telephone itself as opposed to another common type of consensual monitoring, an on-the-body recorder.

Mr. DRINAN. But it involves deception, does it not, or entrapment of the individual speaking to somebody who is your agent?

Mr. DECKER. Did you say entrapment?

Mr. DRINAN. No. I used to teach criminal procedure, so I did not mean entrapment in the technical sense. But, it is a deception and misleading term. In any event, has permission to conduct such monitoring ever been denied?

Mr. MILLER. I do not know how often it has been denied.

Mr. DRINAN. I would like to know if you have any statistics on that subject?

Let me continue. I think you raise a very good point where you say that the Congress has not indicated clearly what it wants the FBI to be, and you allege some inconsistencies on page 34 of your statement between what we want and what you people want. I wonder if you would state those? Could you try to pinpoint the inconsistencies for me?

Mr. MILLER. We realize that the entire area of wiretaps is very controversial. We realize that on the other hand, where authorized, electronic surveillance is an extremely beneficial investigative technique.

We have attempted to analyze each bill before this subcommittee in terms of how it would affect the electronic surveillance operations of the FBI, including consensual monitoring. When we say it appears necessary for Congress to first give full and careful consideration to what it desires the FBI's function to be, particularly in the intelligence area, we view this not as an audacious little investigative agency lecturing Congress in these problem areas; we are merely trying to put important issues in perspective. We know that some of our investigative efforts, particularly in domestic intelligence collection, are extremely difficult to define. In the criminal area, they are less difficult to define because the crimes of violence, kidnaping, and of organized crime are less difficult to define. In the counter-intelligence area our activities are also fairly readily defined.

What we are saying here, Mr. Drinan, is this: That we do not have any hangups on how these procedures should be set up. We do not have any feeling one way or the other that the procedures must be authorized by the Attorney General, for example. All we feel is that there are problems in this country that require different kinds of investigation to resolve. These are problems that affect the ongoing well-being of the United States. However, these problems are worked out, we do not really care as long as—and, as a matter of fact, I have had conversations with Mr. Peterson about how this thing might operate. We know that there has been some criticism about the Attorney General being the man who authorizes warrantless wiretaps, and I told Mr. Peterson that the FBI does not have any feelings, pro or con, that he should be the one to do it. Our

main concern is, that, because the wiretap is a very valuable investigative technique, some effort must be made for all of us to get together on this important issue. And if some committee were set up to oversee the problem——

Mr. DRINAN. This is the committee, sir. If this committee of the House does not do it, then it is not going to be done.

I find it significant that you have not mentioned the word privacy in your testimony or in the questioning. I find it disappointing that an administration whose President speaks about privacy and has appointed a Commission on Privacy, can come forward represented by the Department of Justice and the FBI who have totally rejected every legislative proposal to correct the abuse of wiretapping and electronic surveillance, have made some vague suggestion that maybe in the future you may come forward with a bill, but that is not very helpful to this committee. I thank you for coming.

Mr. KASTENMEIER. The gentleman from Maine, Mr. Cohen.

Mr. COHEN. Thank you, Mr. Chairman.

Mr. Miller, as you can understand, we are very concerned about the serious overtones and implications of wiretaps, also with defining the role of the FBI in solving crime, and as I think you indicated, in preventing it. I, like my colleague, Mr. Drinan. have had some experience in teaching criminal law, and as I recall, two things are necessary for crime. One is the *mens rea*, which is the criminal mind, and the other is the overt act. You get into a very difficult situation when people are just talking about committing a crime and not actually engaging in any overt act to carry it out. This raises in my mind certain Orwellian nightmares about police when the FBI or some other Federal agency tries to determine what people are thinking about or talking about when they have engaged in an overt act. And so, we are very cautious on this committee, as we should be, with our Constitution. We must make sure that the line is strictly drawn between legitimate dissent and the talk of revolution. We are trying to determine what standards have been applied in the past and what kind of a protection can we give to the people of this country.

I think the air, as you have indicated in your statement, has been permeated with a sense of distrust and cynicism about this Government, and there is a great deal of apprehension. And I guess from your statement this is based upon something more imaginary than real, if what you were saying is correct.

I also was interested in your statement in that in the domestic surveillance area you become concerned with bomb throwers and, of course, you may have noticed in the paper, several members of this committee have been accused of being bomb throwers of sorts, and have expressed some apprehension and anxiety that their own offices are being wiretapped. I assume that there is no basis for their fear or apprehension that members of the Judiciary Committee would be wiretapped under the domestic surveillance rationale merely on account of the views that they express? Is that correct?

Mr. MILLER. Certainly not.

Mr. COHEN. We are dealing with wiretaps specifically under this law, but electronic surveillance takes in a great deal more than

simply the wiretap, does it not? And I would assume the FBI has at its disposal a number of very sophisticated devices which do not involve tapping wires or even tape recordings, but devices which are capable of picking up conversations at the end of the room, in another room, without the knowledge of the participants. Does it not?

Mr. MILLER. Well, when you talk about sophisticated devices, I know that there are—from a drawing board standpoint—there are probably a lot of things we would like to do that we are not capable of doing. I think in the electronics area much credit has been given to our investigative and intelligence agencies for capabilities that do not exist.

Mr. COHEN. For example, would the FBI have in its possession devices which could be pointed, let us say, at the far corner of this room to pick up a conversation taking place at the end of this room?

Mr. MILLER. You are talking about devices similar to those that they have in professional football games where they listen to the signals of the people?

Mr. COHEN. Right.

Mr. MILLER. Those devices are conceivable.

Mr. COHEN. Not conceivable. Do you have them, and do you use them?

Mr. MILLER. I do not have the technical capability to discuss our state of the art.

Mr. COHEN. I guess what I am trying to get at might fall beyond the range of our general discussion about wiretapping, someone putting a physical interceptor on a telephone wire, but what I am talking about is this whole realm of investigation of privacy, the Government trying to prevent crime from taking place. Do we have the type of sophistication that would simply pick up conversations? It is readily available to CBS, NBC, and ABC, and I assume the FBI must have similar devices.

Is that correct?

Mr. MILLER. As I say, I do not know what our state of the art is in that particular area. What I can say is this: If we were using any kind of a device like that, then I most certainly would be asked for the authority or permission to use it. I have never been asked by anyone to use that kind of a listening device. We just do not use them. We do not see the necessity for it in a one to one situation where we would have a desire to know what one of the people is talking about. For example, one of the most vicious crimes that we have in the United States today is the extortionate credit situation whereby the time the case comes to us, the victim, in his own mind, feels he is heading towards his last few days. Now, in a situation like that, the best kind of a device that we would use would be a consensual monitoring of a telephone, and the other would be a body recorder on the victim. Now, rather than trying to go out to some meeting place and aim something at a group, we would take this other route instead. It is a far more effective investigation technique than the kind of a listening device you describe.

Mr. COHEN. Then is it fair to say that——

Mr. MILLER. If we have them we do not use them, and I do not even know that we have them.

Mr. COHEN. Is it fair to say that you do not think you have any such device, but if you did it has never been used to your knowledge, or to the knowledge of any of your associates in the field of domestic or foreign intelligence? Is that correct?

Mr. MILLER. Yes.

Mr. COHEN. I am inquiring, here, because it does not seem to be specifically covered by our general discussion of wiretapping when we are not dealing with the wire itself, and I was interested in your statement that people who might be listening in or overhearing conversations at some point make the subjective judgment as to which conversation may stay in or be deleted.

For example, I think you mentioned in discussing the attorney-client situation that someone could be overhearing a conversation and would recognize a voice as the attorney for the Chicago Seven or someone and, therefore, the monitor would be turned off. And I am just wondering from a technical point of view how you gather this information? I assume it is on tape recordings?

Mr. MILLER. Yes.

Mr. COHEN. Are they then transcribed?

Mr. MILLER. In part.

The pertinent portions are transcribed, but all the conversation is available.

Mr. COHEN. This carries significant overtones in other areas with which you may be familiar. Are they edited, for example?

Mr. MILLER. There is a particular purpose for every wiretapping situation. Portions of intercepted telephone conversations pertinent to a subsequent trial or presentation of facts to the U.S. attorney are transcribed from the tape. The whole tape is maintained. We maintain the tape, and that tape can be replayed to see what it does have on it at any time, but only the pertinent portions are originally transcribed. There may be "Bring home a dozen eggs" types of situations which would not be pertinent, and these are not transcribed.

Mr. COHEN. Well, as I understand it then, the FBI does try to maintain a very strict adherence to confidentiality, the right of privacy, and the recognition of certain privileges such as the attorney-client privilege? How about physician-patient privilege?

Mr. MILLER. The same. Any kind of a privileged situation.

Mr. COHEN. So that what would apply too, for example, to the Ellsberg situation, Ellsberg-Fielding, that would be a private conversation between a doctor and his patient, which would not be of interest to the FBI or anyone in trying to determine what Mr. Ellsberg is saying to his doctor, is that correct?

Mr. MILLER. Yes, that is correct. We did not have a wiretap on Mr. Ellsberg.

Mr. COHEN. And had you had a wiretap on Mr. Ellsberg, or possibly his physician, any information that had been relayed or related by Ellsberg to his physician would have been deleted or simply not monitored?

Mr. MILLER. Well, we did not have one.

My guess would have been, that the agent who was doing the monitoring would have considered that a privileged situation.

Mr. COHEN. Would it have been the judgment of the FBI that it would have been illegal to monitor that conversation, or simply a recognition of a privilege?

I mean, is it not just as much of interest to you in investigating espionage, or foreign intelligence or domestic intelligence cases, as to what that person under suspicion might be saying to his doctor or his lawyer?

Mr. MILLER. Well, there you get into a matter of judgment. If it were an espionage case—if a spy were talking to his doctor—prosecution in that situation would generally not be your end goal; however, if prosecution were the thing that you had hoped for or had in mind, and the intercepted conversation went to the heart of the case, the agent may well go ahead and record the conversation, but then notify the United States Attorney so that whatever necessary precautions to preserve prosecutable case could be taken. For example, sometimes in a title III case, conversation may be recorded and just before the conversation is terminated the identity of the parties becomes known to the agent. But, there it is already recorded; then, we go to the U.S. attorney and explain what happened and the U.S. attorney will generally say seal it. And that is how it is handled where there is an accidental overhearing of a privileged conversation.

Mr. COHEN. But as a matter of policy though, the FBI would never engage in wiretap or electronic surveillance of conversations between an attorney and client or doctor and patient? Is that a fair statement?

Mr. MILLER. Well, when you put the word never in there—we would not want to do it, unless the facts and circumstances of the situation were such that would——

Mr. COHEN. To your knowledge has it been done?

Without getting into the specifics.

Mr. MILLER. No, I do not know of any case.

Mr. COHEN. What percentage of the requests for permission to apply for a court ordered surveillance are disapproved by the Criminal Division of the Justice Department?

Mr. MILLER. By the Criminal Division?

Mr. CLEVELAND. We had 112 court orders in 1973, and there were 28 additional ones turned down by the Department of Justice.

Mr. COHEN. 28 requests?

Mr. CLEVELAND. Yes, 28 were turned down; 112 were approved.

Mr. COHEN. Just a couple more questions, and I suspect that you do not have all of the answers. But, if you do I would like to have them for the record and if not, perhaps you can furnish them at a later time. But, how many of the wiretaps—I would like to go through the tests that have been used by the Supreme Court—are related to protecting the Nation against actual or potential attack, or other hostile acts of a foreign power? That would be one category I guess you would have some wiretaps. Second, to obtain foreign intelligence information deemed essential to the security of the United States. Third, to protect national security information against foreign intelligence activities. Fourth, protecting the United States against overthrow of government by force or other unlawful means, and, five, against any other clear and present danger to the structure

or existence of government. Would you be able to give us a breakdown on those? Not now, but at some other time?

Mr. MILLER. As I indicated, the answer to some of those questions most certainly can be furnished.

Mr. COHEN. Thank you very much.

Mr. KASTENMEIER. May I inquire of the gentleman from Maine, and perhaps Mr. Miller as well, with regard to the five categories you gave, which seemed very useful, are these identifiable categories that are actually used?

Mr. COHEN. These are the tests that are used by the court under the act, I believe.

Mr. MILLER. Yes.

Mr. COHEN. I believe that three and four are probably negated by the *Keith* decision, but I would still like to have the information.

Mr. MILLER. Yes.

Mr. KASTENMEIER. Incidentally, amplifying the gentleman from Maine's question, what percentage of all taps conducted or authorized by the Bureau involve investigation under criminal statutes versus either counterintelligence or foreign intelligence gathering, or what would have been domestic intelligence gathering?

Mr. MILLER. All title III surveillances are criminal.

Mr. KASTENMEIER. Yes.

Mr. MILLER. Every one of them.

Mr. KASTENMEIER. Right. And how many Federal warranted wiretaps are there versus warrantless taps?

Mr. MILLER. Well now, we are talking about numbers again and the number that Mr. Peterson gave you yesterday would be our response. Does that——

Mr. KASTENMEIER. I do not recall. I think there are numbers that were available for a certain class. Actually, I was asking only for a ballpark response in terms of the substantial majority of taps conducted. Are the substantial majority of taps conducted under title III?

Mr. MILLER. Well, I think Mr. Cleveland said 112 were authorized in 1973. Now, these generally would be wiretaps which were on for a period of only a few days. In the other area, intelligence gathering, as Mr. Decker indicated some of these would have been employed for a period of quite some time, so it is difficult to compare the use of title III wiretaps with the use of warrantless wiretaps for national security purposes, because they are really two different animals. Incidentally, all of the wiretaps in the national security area are submitted to the Attorney General every 90 days for reauthorization.

Mr. KASTENMEIER. It may be more productive to try to get the figures from the Attorney General on that question.

Let me ask you then, is there more activity in terms of wiretapping and electronic surveillance, in the title III area than in the area outside of title III? I'm talking about authorized areas in the Federal System?

Mr. MILLER. Are there more in the title III area than in the non-title III area?

Mr. KASTENMEIER. Right.

Mr. MILLER. I would say that they are generally comparable.

Mr. KASTENMEIER. They are comparable?

Mr. MILLER. Yes.

Mr. KASTENMEIER. Under title III, what percentage would you identify as connected with organized crime?

Mr. CLEVELAND. Most of them are organized crime cases.

Mr. KASTENMEIER. Most of them are?

Mr. CLEVELAND. Yes.

Mr. MILLER. The figures in my statement indicating the productivity of title III, reflect that out of 2,700 organized crime arrests, 1,700 of them were attributable to title III surveillance.

Mr. KASTENMEIER. I have just one other line of questions, and this has to do with the policies governing overhearings. What system does the Bureau have for indexing overhearings?

Are title III and national security cases treated differently?

Mr. MILLER. No. They are treated primarily the same, Mr. Kastenmeier. The indexing procedures are standard. The material is reviewed by a case agent, and he would determine what was pertinent to the situation he is investigating, and if it is pertinent then he would index it.

Indexing makes the material retrievable, as I indicated to Mr. Smith. In a legal proceeding, if the defense and usually it does, asks the FBI or the Department of Justice if the defendant or his attorney have ever been overheard on any kind of an electronic surveillance, we would be able to determine from a review of our records whether or not the individuals had ever been overheard. If they had then we advise the Department. The Department handles the matter in camera with the judge. If the judge feels that this information is necessary to the defendant for his defense, then the information is furnished to him.

Mr. KASTENMEIER. Thank you.

Mr. DRINAN. Mr. Chairman?

Mr. KASTENMEIER. Yes. I yield to the gentleman from Massachusetts.

Mr. DRINAN. One last question. Mr. Miller, I assume that the FBI or another agency regularly collects intelligence from foreign embassies in Washington. May I ask, on the assumption that this is done and it seems to be accepted that it is done, does another agency sometimes alert the FBI to wiretap evidence that they have acquired as to some potential crime that might be forthcoming?

Mr. MILLER. Would another agency alert us to a situation that they felt we would be interested in? They would; yes, sir. We, in the intelligence community, all of the intelligence agencies in the United States, the State Department, the CIA and so forth, cooperate very closely on intelligence matters.

Mr. DRINAN. The tap that the CIA or someone else might have on the Russian Embassy, that is not included in the number of taps that you have given to us, is it?

Mr. MILLER. Well, the CIA would not——

Mr. DRINAN. I am sorry, some domestic agency, or would it be the FBI?

Mr. MILLER. It would be the FBI. Anything domestic would be the FBI, yes, sir.

Mr. DRINAN. And in the number of wiretaps of a quasi-permanent nature, that you mentioned, would the wiretaps to the embassies be included?

Mr. MILLER. Well, we are talking about numbers.

Mr. DRINAN. What? Numbers, yes.

Mr. MILLER. You are talking about numbers.

Mr. DRINAN. Plain old numbers.

Mr. MILLER. The numbers——

Mr. DRINAN. That you gave to Mr. Kastenmeier.

Mr. MILLER. These are the total numbers.

Mr. DRINAN. That would include——

Mr. MILLER. These are the total numbers.

Mr. DRINAN. And every 90 days I understand that somebody sends a piece of paper to the Attorney General and he approves the continuation of these wiretaps on the embassies?

Mr. MILLER. I would prefer in discussing this particular type of thing to brief you in closed session, Mr. Drinan.

Mr. DRINAN. All right. Thank you. I yield back to the chairman.

Mr. SMITH. Mr. Miller, in title III wiretaps it would seem to me that once in a while some incriminating evidence against people who are outside of the court order, people who drifted into the conversation someplace would be overheard.

Are cases ever built against people who are casually overheard on an authorized wiretap?

Mr. MILLER. Let us take, for example, a court-authorized wiretap on a certain telephone instrument. Let us say it is on an illegal gambling operation. We do not know at the time that wiretap is authorized, everybody who is going to be a part of this network of crime. Now, it is entirely possible that in addition to the people whom we identify in our application as being involved in this situation, there are others involved. Part of the effect of the wiretap itself is to identify others who may be involved. So, to identify individuals who are part of the $30,000-a-day operation, it can. But, then they are handled under separate considerations in ongoing investigations. They can be drawn into the network. That is why, in many instances following one of these kinds of electronic surveillances, you will have a situation where there are 65 arrests growing out of one title III wiretap, and I am sure at the time that the thing was authorized, we did not know all of the 65 people were going to be a part of it. But, in his prosecutive opinion, the U.S. attorney feels that enough probable cause has been developed both from the wiretap and follow-up investigation on which to base a warrant for the arrest of all of these individuals.

Mr. COHEN. Would the gentleman yield?

Mr. SMITH. Thank you. Glad to.

Mr. COHEN. Just to elaborate a little bit further about the incidental caller or the casual caller on one of these wiretapped phones, would it be that you would continue to have this man or this woman's name in the record, however you may not use it for any prosecution of that individual at that time, but even though it was an incidental caller on an unrelated matter and even a noncriminal matter, that

caller's name as I understand it, remains in the fiile, and I assume you have computerized filing systems, do you not?

Mr. MILLER. No.

Mr. COHEN. You don't?

Mr. MILLER. We do not. Our electronic indices are not computerized. We cannot assume——

Mr. COHEN. I just say that I am a little bit surprised at the lack of sophistication in the FBI systems where you do not even have equipment which is equivalent to that of CBS or NBC or ABC at your disposal nor do you have computerized records so that you can call a man's name or a woman's name up at a moment's notice to search back over your records or tapes and transcripts and so forth. I am rather amazed at that, but I am sorry. Go ahead. Why don't you answer.

Mr. MILLER. Well, in answer to your question. I did not say we didn't have the equipment at our disposal. Certain equipment can be used to do certain kinds of jobs, but if the equipment is not necessary to perform a certain type of investigation then there is no real need to have the equipment. On the matter of automated indices we do not have them. We do not feel it is necessary to have them. It is not that gigantic a proposition. It can still be handled very, very easily manually.

And now, in answer to your first question—you cannot necessarily say that an incidental caller's name is going to be indexed. It may or may not be. That is a judgment on the part of the case agent. If it is the corner grocer, or the minister, or else who clearly does not have anything to do with the actual investigation, his name probably will not be indexed, but he will be on the tape which is preserved. However, for all intents and purposes his identity is not with us unless the tapes were replayed.

Mr. COHEN. Let me just go back over this to clarify the record if we could. As I understand what you are saying, the FBI does not have the sophisticated equipment at its disposal? You do not have the type of equipment that I was talking about with these zoom microphones or whatever they want to call it, the boom microphones, you do not have that?

Mr. MILLER. We do not have a need for it.

Mr. COHEN. No. Do we have the equipment itself?

Mr. DECKER. I do not know of any.

Mr. MILLER. I do not know that we have that equipment. I do know similar equipment is available, just like these directional football devices to listen to the signals.

Mr. COHEN. Well, the FBI does not have it in its stockpile, let us say, of information gathering devices. They are readily available on the open market to commercial networks, but you do not see the need to resort to this type of sophisticated listening device, correct?

Mr. MILLER. Yes. If it were necessary I am sure that we would.

Mr. COHEN. And therefore, you have not done so in the past and do not foresee doing so in the future?

Mr. MILLER. Well, I cannot say that we do not—many of the things we hear discussed are in the technical dreaming stage, and in the

realm of, "Would it not be nice to be able to do such and such." But, we have not done that.

Mr. COHEN. The only reason I am pursuing this is because we are being called upon to draft legislation and in drafting it I want to be sure that we take into account every possibility.

Mr. MILLER. Yes.

Mr. COHEN. While sitting on another subcommittee, when one of the members of the Justice Department testified before us last week, that I asked hypothetically, if the chairman of the subcommittee were on an enemies list as someone who was hostile to a particular interest in this country, and if I had a conversation with him, or were seen socializing with him, would my name go in the file as well, and the answer was it probably would. And I suspect this is the line of questioning that is being developed here. When you have the casual caller calling up on a wiretapped phone, and records are maintained permanently, his name is on those records or in the transcripts where transcripts are made. You are building up files on incidental calls which may be used in the future. And what we are asking is, are there any limits or can we define limitations upon the proliferation of people who are under surveillance? We do not have any guidelines other than the individual judgment of the FBI agent, and we have to consider whether we can draw enforceable standards to deal with this situation.

Mr. MILLER. That is the only way thus far that we have been able to handle this situation. In drawing guidelines, you still get back to the judgment of the individual who is doing it—whether the material is pertinent or not pertinent. And please understand, these are professional people, schooled in their work, who are supposed to be able to make a determination of relevancy.

Mr. COHEN. Thank you.

Mr. KASTENMEIER. On behalf of the committee, Mr. Miller, we wish to thank you and your colleagues for appearing this morning.

These 2 hours have been very productive and you have been very patient and we appreciate the contribution you have made.

Undoubtedly there will be further need for us to get together, and we will leave that to the future. And in the meantime, the subcommittee would appreciate your fulfilling the request of the gentleman from Maine. Your response should be directed to the subcommittee.

Thank you very much for your presentation this morning.

Mr. MILLER. Thank you, sir.

Mr. KASTENMEIER. Next the Chair would like to call Mr. William Bender, director of the Constitutional Litigation Clinic at Rutgers University School of Law in Newark, N.J.

Mr. Bender has represented clients in numerous cases involving national security electronic surveillance and wiretapping. The hour is late, but nonetheless, Mr. Bender, we appreciate your appearance.

You have a prepared statement which you may read, or if you desire, you can summarize it, either way, it is up to you.

Welcome to the subcommittee.

TESTIMONY OF WILLIAM J. BENDER, ESQ., ADMINISTRATIVE DIRECTOR, CONSTITUTIONAL LITIGATION CLINIC, RUTGERS UNIVERSITY SCHOOL OF LAW, NEWARK, N.J.

Mr. BENDER. Thank you, Mr. Chairman. And I am sorry for my delay in arriving here this morning. I was tied up in the Monday morning airport syndrome.

I think I would begin by reading part of my statement and if it becomes laborious I will stop and then I would be glad to try and answer any questions the subcommittee may have.

First, I welcome the opportunity to appear before you today and to relate some of my experiences with electronic surveillance matters in several cases, both civil and criminal, in which I have appeared as counsel. The cases include the following: *United States* v. *Ahmad*, which was the *Harrisburg Conspiracy* case; *United States* v. *Ayers*, which was the *SDS Conspiracy* case in Detroit; *In Re Dellinger, et al.*, a contempt case arising out of the Chicago Seven conviction; *United States* v. *Butenko*, which I am presently handling, a criminal espionage case in the district of New Jersey; *United States* v. *United States District Court*, which as we all know is now over; and *Dellinger, et al.*, v. *Mitchell, et al.*, a civil action in the District of Columbia arising out of the disclosure of wiretapping in the Chicago Seven Case in June of 1969. *Sinclair* v. *Kleindeinst*, and that is a civil action arising out of the disclosure in *U.S.* v. *U.S. District Court*; and *McAlister, et al.*, v. *Kleindienst*, a civil action arising out of the disclosure in the *Harrisburg Seven* case.

I shall attempt to create a composite picture for you of the governmental abuses of first and fourth amendment and statutory rights from the public records of wiretap matters in these cases. Based on these experiences, I urge you to reject legislation which provides for so-called national security investigatory electronic surveillance of any kind in both foreign and domestic concerns. I will leave the debate on the constitutionality of prosecutorial surveillance authorized by prior judicial warrant to others. However, I do want to suggest that if the privacy guarantees of the fourth amendment are to be meaningful, the Congress must legislate meaningful administrative controls for the conduct of such prosecutorial surveillance. These controls must be implemented vigorously by the legislative branch.

Mr. KASTENMEIER. When you mention prosecutorial surveillance, you are talking strictly about criminal or Title III wiretapping?

Mr. BENDER. That is right. I am talking about that surveillance wherein the law enforcement agencies have sought permission to wiretap in order to gather evidence or the fruits of their surveillance activities to further the prosecution of crime.

Now, it strikes me that the most serious revelation in these cases I have handled has been the discovery that the Government has intentionally sought to mislead the Federal courts into believing that national security electronic surveillance was for investigatory, intelligence gathering purposes as contrasted with the prosecutorial electronic surveillance which is utilized to gather evidence. And I just want to read, if I may, some of the comments by the Assistant Attorney General, Robert Mardian, made during the *Keith* case, in the

U.S. v. *U.S. District Court* case, which are typical of the comments made in the dozens of cases that I am aware of, and all of the cases in which I have been involved. And then I want to point out, if I can, the stone cold reality of what has gone on in these cases, because it is here where I believe one of the largest abuses is to be found.

Mr. Mardian put it thusly:

> This gathering of information is not undertaken for prosecution of criminal acts, but rather to obtain the intelligence data deemed essential to protect the national security. (Government's Brief, at 16)

Mardian added:

> We stress once again that, in conducting such national security surveillances, the Attorney-General is gathering intelligence information for the President, not obtaining evidence for use in criminal prosecution. (*Id*, at 19)
>
> Moreover, unlike the traditional searches made pursuant to warrant that magistrates issue upon a showing of probable cause, national security surveillances are not designed to obtain facts needed in a criminal investigation, but to obtain intelligence information.

Mr. KASTENMEIER. If it is agreeable to you, Mr. Bender, we will have a 10 minute break so that members of the committee can answer a quorum call on the floor, and we will return directly and resume at 12:25.

Mr. BENDER. I am at your disposal.

Mr. KASTENMEIER. At this time the committee will be in recess.

[Short break.]

Mr. DRINAN [presiding]. Would the meeting please come to order.

I am happy to resume this hearing and to ask Mr. Bender, in the absence of the Chairman, to proceed.

Mr. BENDER. Thank you, Mr. Drinan.

When the *Keith* case finally reached the stage of oral argument before the Supreme Court, Assistant Attorney General Mardian again asserted that the case was not one, "where electronic surveillance was authorized for the purpose of obtaining prosecutive evidence in a criminal proceeding" or a case "where the defendant was the target of the electronic surveillance which was authorized."

I have quoted at length in my statement from the continuing assertions in the same vein, and I will not read them all into the record here. But, the point was clearly and simply made. I think the important thing for this committee to realize is this argument was universally made in all the cases, both foreign and domestic, where the Nixon administration chose to admit to electronic surveillance in recent criminal cases and submit the legality claim to the test in litigation. For example, before the trial the Government in *Ahmad*, "admitted to what * * * [it] believe[d] are probably conversations of Sister Elizabeth McAlister, one of the defendants in this case," and conversations having been overheard in a national security electronic surveillance authorized by the Attorney General of the United States [hearing of May 24, 1971, pp. 56–57]. The Government steadfastly maintained from the outset that the overhearing of Sister McAlister was inadvertant, having nothing to do with furthering the prosecution of its case and having no relationship to trial evidence [T.78].

The Government's earlier representations, that whatever illegal electronic surveillance—of the so-called national security variety—it

may have conducted was only for intelligence data gathering, were promptly contradicted. FBI agent Smith, who initiated the request for the surveillance in question [Hearing of May 2, 1972, partial transcript p. 31], and then supervised the surveillance operation [T. 36], testified in direct opposition to the prior representations of the Government attorneys; and almost the first words out of his mouth were very clearly and unequivocally stated; the surveillance was conducted to gather evidence to further the prosecution in this case [T. 24, 45, 47].

The same can be said for the *Ayers* case, and I have set forth some of those facts in the statement.

Now, after almost 5 years of civil litigation in the *Dellinger* case, which I cite on the first page of the statement, the Government has turned over the requests for surveillance of the national security variety and authorizations for those surveillances wherein the Chicago Seven defendants were heard, and other specific organizations that were parties to the litigation.

I am bound by a protective order not to reveal the contents of those documents before this committee. However, I want to strongly urge that before this committee considers any specific legislation that it take up Mr. Miller of the FBI and the Department officials on their offer, and in Executive session ask for and examine those documents. The actual inter-departmental correspondence on specific surveillances, which I have seen, all the surveillances I have seen, contain references to the intention of using the surveillance for prosecutive purposes. The specific crimes which were sought to be investigated and the person to be investigated, and the prosecution to be mounted, are all set forth in infinite detail, and I would suggest as strongly as I know how, that you ask for and examine this documentation.

What I am suggesting is that the claim of investigatory surveillance is a ruse, and it is a ruse which the Government used in order to attempt to win the power which the court repudiated in *U.S.* v. *U.S. District Court*, and which it again is bringing before this Congress with regard to the foreign security surveillances to which some of the legislation before this committee refers. And I would suggest that this committee has got to pierce the claims in both areas if this legislation is going to be meaningful.

Mr. DRINAN. Mr. Bender, if I may follow up on that for a moment. If we do not have the votes for the total abolition of this type of surveillance, how can we regulate it?

Mr. BENDER. Well, I believe you have to regulate the process by which the agents conduct all surveillance. In other words, specific records have to be designated by the legislation, and what the agent does, by way of requesting an authorization, how the authorization comes back, and then how the delegation to conduct the tap is made, has got to be specified by the legislation in specific detail, and then what the agents do when they conduct their surveillance has got to be memoralized in specified writing. So, for example, the following cannot occur: An agent conducting a national security tap sits with earphones on his head, and a tape recorder in front of him, and a radio microphone by his side, and he overhears a conversation con-

cerning a criminal transaction. And he has the capability of directing agents in the field to take investigatory action based on what he has heard over the tap. Thereafter, he may or may not make a cut on the tape or contemporaneously make an entry in a log or send out a formal lead through an airtel. But, the fact of the violation of privacy has already occurred, and then after the fact, in the criminal case or in a civil case, when it is attempted to put it all back together again, it is almost an impossible task because the whole record keeping system has been designed to obliterate, at least in terms of criminal process, the critical violation. So, I would suggest that you have to have a housekeeping committee of the Congress, of the House or of the Senate Judiciary Committees, and that the activities of the agents conducting all surveillance has got to be scrutinized, subjected to periodic review, and the legislation ought to specify that if any agent transgresses from the prescribed train of events, does not use the forms, does not specify the requisite information on the memoranda, then he loses his job.

And that has got to be an offense, and I believe whatever the legislation is, that is the only way to ensure that in the administration of legislation there will not be any abuse.

Mr. DRINAN. Mr. Bender, do any of the bills under consideration, mentioned in the opening of your statement, approximate what you are suggesting now?

Mr. BENDER. I have not seen that in any of the legislation that is before this committee now, and I am suggesting it as an addition.

Now, I do not want to be understood to suggest that I am in favor of bills which authorize surveillance. I am not. But, if we are dealing in the practical world where either a version of Title III surveillance for prosecutive purposes, or a version of a bill allowing for investigatory surveillance in the foreign area is to be provided for, then to make the guarantee reasonable, we have to close the loopholes and find a way of regularizing the conduct of the officials who administer the legislation.

Mr. DRINAN. Mr. Kastenmeier's bill attempts to do that by restricting the number of days that the wiretap can be installed, and Mr. Kastenmeier can speak to that, but I think that is an approach, that it is 15 days and then it follows to 10 days on the renewal. Now, do you think that that is a welcome approach to stopping this open-ended surveillance, as they were talking about this morning?

Mr. BENDER. Absolutely. I would limit it as to time and I would limit it as to scope and direction. And it would also have to regularize what happens during the 15 days so as to be meaningful.

Now, this is not to suggest that the only problem flowing from electronic surveillance is the problem of tainted evidence in a criminal case. Not so at all. The invasion of constitutional privacy occurs whenever the overhearing takes place, and somebody else hears someone else's thoughts or words. But, the window into the problem that I have seen is when the government chooses to admit to electronic surveillance in the criminal case and that is——

Mr. DRINAN. If the Congress is unable or unwilling to establish all of those specified limits that you suggest, could the courts do it?

Mr. BENDER. The difficulty is that after the fact there is no real way of enforcing such requirement. After the fact you are taking testimony on cross-examination from agents in a taint hearing and the agents are attempting to show, to sustain the governmental burden that the government has an independent source for its evidence, and it is in the adversary proceeding where one party is trying to save the case; namely, the government, and the other party, the defendant, is trying to kill the case by either finding taint throughout the investigation, or taint of particular trial evidence. So, I do not think in these circumstances the adversary system is necessarily the best way of regularizing the conduct.

It is no secret that there are virtually no reported cases where federal courts have found taint following electronic surveillance, and when one contrasts that fact with the experience of finding taint in the whole other realm of violations of the fourth amendment, I find it somewhat astounding. I do not believe, by the way, that it is the product of there being no taint. I think it is the product of a system which is clandestine in nature, and where the facts are controlled by the agents engaging in the illegality in the first place.

Mr. DRINAN. Thank you. I yield back the Chair to Mr. Kastenmeier.

Mr. KASTENMEIER. Mr. Bender, did you want to continue?

Mr. BENDER. Yes. Let me pick up with a few sections of my statement, and I will make myself available to the committee for questions. I am looking at page 6 now in the middle of the page.

Interim disclosures by the government in the *Ayers* case, that is the *SDS Conspiracy* case in Detroit, reveal the enormity of some of these problems and the difficulty of getting at the truth in the context of a criminal prosecution suppression proceeding.

United States v. *Ayers*, No. 48104, U.S. District Court, Eastern District of Michigan, Southern Division, was a conspiracy prosecution of the Weathermen faction of the Students for a Democratic Society; the case was dismissed by the court on October 15, 1973.

The Government moved to dismiss this case because of its unwillingness to suffer the revelation of the identity in adversary hearings ordered by the court of an agency that had admittedly conducted some of the illegal surveillance activities.

However, pursuant to an interim order on June 4, 1973 by Hon. Damon J. Keith for disclosure of illegal electronic surveillance, the Government turned over to the defendants 3,000 pages of transcripts of telephone conversations covering eight months of surveillance. And these were surveillances where the government conceded that the defendants had standing and othrwise were entitled to disclosure following the Opinion of the Supreme Court in *U.S.* v. *U.S. District Court*. However, the Government asserted that these transcripts represented full compliance with the interim disclosure; namely, those surveillances covered by *Keith*. Although the judge reserved decision as to whether or not the defendants had standing to receive summary logs of the overhearings made during this time period, in the large carton with the 3,000 pages of transcripts, and we inspected those logs prior to returning them to the government, an inspection of these logs by the defendants indicated that the Government was

either unwilling or unable to comply with the interim disclosure order concerning surveillance even where illegality and standing were conceded. The logs listed 500 overhearings during the 12-day period; in the 500 overhearings 239 parties were listed as "unidentified" by the government. Upon inspection, defendants were able to determine that a number of these unidentified overhearings were of the defendants themselves and at least eight were of their attorneys. In each of these instances, no transcripts of the illegal overhearings were provided by the government to the defendants.

Now, in the ensuing proceeding, we debated with the government the numbers of our projections as to the size of this problem. We estimated that at any time the Government was unable to formally identify for record keeping purposes one-half of the participants. The Government said that our arithmetic was somewhat overblown and it was more like 10 to 20 percent, at which point we said we will concede that it is only 10 to 20 percent, and in a criminal case it makes absolutely no difference. The Government has got to disclose all instances of illegal overhearings pursuant to *Alderman* v. *United States*, and it has created a system, a record keeping and disclosure system, which is designed to do, or at least accomplishes, exactly the opposite.

In the *Ahmad* case, also in the *Ayers* case, and I am looking now at page 9 at the bottom, we began to flush out some of the mechanics of how this system fails in its disclosure responsibility.

In the *Ahmad* or *Harrisburg conspiracy* case the tentative determination of the participation of Sister McAlister on the calls was surmised by the Government by reference to the telephone numbers that they were called by the subject of the surveillance [T.12], namely the number of the convent where Sister McAlister then resided along with other nuns. However, no effort was made to identify the voice of any person calling into the tapped location during the course of the surveillance or afterward [T.14]. Unless a full name was mentioned in the course of a tapped conversation, the only means of identification was by way of the name of the phone service subscriber to whom the intercepted call was made [T.14]. FBI Agent Smith recognized that often in phone conversations, a full name is not used. So, even in the case where the Government made disclosure, they were unwilling to make the formal assertion of identification. Now, this is not to say that when agents are monitoring a live tape recorder in front of them, and they have earphones on their head, and a microphone with which they can communicate with an agent in the field, that they do not indulge in the luxury of tentative identification. With the agent investigating Sister McAlister in the *Harrisburg* case, he hears somebody who he thinks is Sister McAlister say "I am going to the airport and meet so and so", and although he cannot say this is Sister Elizabeth McAlister, he does pick up his microphone and direct a field agent to get out to the airport and see if McAlister shows up. But, then, in concluding the summary log, because I do not have the full name or the ability to make a meaningful identification, he just might write down "Liz, last name unknown", or a phonetic spelling of a name, or "unidentified call placed, unidentified person". And he may not even bother

to reflect on the log of his own activity the investigatory lead or the airtel or some other writing that he has used in the surveillance that he has overheard in order to further the criminal process. And then in the ensuing taint hearing where the facts are known only to the government, and the only power the defense lawyer has is to cross-examine the agent as to what he did, and the records are denuded of this kind of reference, then the task is impossible.

Now, I suggest to you once again that in the items we saw in the *Dellinger* records, which as I indicated earlier I cannot read here because of the protective order in *Dellinger* v. *Mitchell*, there is a concerted effort within the FBI to protect the confidential source in the manner I have just suggested. There are specific documents where agents are told to avoid—and I would love to quote these documents here today—but to avoid, to use my own words, the lamentable, practice of revealing the existence of illegal sources of internal reporting documents for justice reasons and in the same vein there is also reference made to the practice of characterizing surveillance, many surveillances, under one recording system to minimize the reporting of the extent of the program. There are documents which would indicate an effort to overemphasize the foreign involvement of certain organizations and minimize the domestic activities of the organizations. And these documents are contemporaneous with litigation in the courts concerning the very foreign security power which this committee and its chairman are concerned with and proposing legislation. I suggest to you as strongly as I can to probe the specific practices before you consider legislation. And I have kind of listed the series of questions which I would urge upon you in making those examinations of records and I would like to read those into the record and then close my statement.

And this I think is what this committee should find out.

1. How are agents of the FBI instructed to circulate facts during an investigation which are gleaned from an electronic surveillance source? Testimony in some cases and recently revealed specific documentation in materials covered by protective orders will show elaborate efforts to conceal electronic surveillance sources. This practice makes a showing of taint extremely difficult and insulates illegal activity from even internal Justice Department controls.

2. How are electronic surveillances numerically counted and described to the legislative and judicial branches? These materials will show efforts to conceal the extent of national security electronic surveillances by grouping many surveillances under a specific reporting heading.

3. How has the Justice Department sought to analyze the foreign and/or domestic character of its national security surveillance? These materials will show an attempt to overemphasize the contacts and involvement with persons in foreign countries by the subjects of certain surveillances to support arguments in court of the foreign security character of the electronic surveillances in question.

4. How extensive has national security surveillance been? Disclosed materials would indicate that the program was far more extensive than anything indicated in Department of Justice statistics.

5. What are the constitutional consequences of the national security electronic surveillance program? Materials already disclosed indicate a surveillance program of breathtaking enormity involving hundreds of thousands of overhearings, authorized on fear, innuendo and speculation without regard to the privacy rights and rights of association and free speech of a free people. The program is the consequence of raw executive power, unchecked by this legislature or the judiciary. To legislate against and then to control these abuses a full investigation must be undertaken and specific review procedures established.

I close these remarks by asking you whether these past 2 years, characterized as they were by the constant invocation of the specter of threats to national security for all necessary occasions will foreclose the meaningful pursuit of your task. I would hope that recent history suffices to demonstrate that the shopworn talismanic incantation "national security" can no longer foreclose democratic processes. A good beginning would be full scrutiny of the entire national security electronic surveillance program and the legislation of substantial controls to prevent its ugly reoccurrence.

Mr. KASTENMEIER. Thank you, Mr. Bender, for a very helpful statement. I think as a matter of fact, if anything, the questioning by this committee has indicated its interest particularly in warrantless taps, or that done under the guise of national security, because this seems to be the most murky area. But, I understand you to suggest that tapping or surveillance conducted in behalf of intelligence gathering, was all right, except in that it might from time to time be used against individuals for prosecutorial purposes. This suggests that you were not unwilling that wiretapping and surveillance be used for intelligence gathering as long as it is not used against individual defendants in criminal proceedings.

Mr. BENDER. I hope I did not give that impression. I am absolutely opposed to intelligence gathering surveillance. As Justice Powell suggested in *District Court*, intelligence gathering surveillance is the Executive writ, it is the all-sweeping, all-encompassing effort to know what a large group of people are doing. It is as abusive in and of itself as any violation of the fourth amendment, and I see no difference between intelligence surveillance of either domestic or foreign concerns and a program of mass searches of houses and mass interrogations. I do not want to leave that impression with committee at all.

However, what I am trying to suggest is that in advocating intelligence surveillance, this Administration was attempting to hoodwink, I believe, both the legislature and the judiciary and they did not mean by intelligence surveillance what they said they meant. They specifically represented that they meant the program which the Supreme Court rebuked because there were no standards. I think we can demonstrate beyond cavil that what they did mean was a program of gathering of evidence to prosecute when they had no probable cause, no foundation for the tap at all. Now, this is not to say that they did not want the intelligence data as well, that the Government did not want to know everything SDS was doing or everything the Panthers were doing or everything a variety of other

organizations were doing for its intelligence value. But, in the specific documentation which we have seen, the justification is that we want to know in order to be able to prosecute so-and-so for a particular crime. And in the documents where the surveillances are justified for periodic review, there is a process of bragging about the prosecutorial successes as these surveillances, which tend to go on for a long, long time. So, I want to suggest that we abandon investigatory surveillance because it is constitutionally abusive no matter how it is described, because it is not founded upon probable cause. And because it is a ruse for prosecutorial surveillance at all we control it in the most tight and careful manner possible knowing that the program, unless it is controlled, is going to be abused.

Mr. KASTENMEIER. Toward the end of his statement this morning, Mr. Miller characterized the three areas of wiretapping and surveillance as: one, the criminal area under title III where warrants are obtained, two, the counterintelligence or foreign intelligence-gathering field for which warrants are not obtained, and three, the field of domestic intelligence. And he suggested that pursuant to the *Keith* case they were not presently engaging in any wiretapping to obtain domestic intelligence. Presumably under title III they could engage in domestic intelligence wiretapping but he suggested two problem: one, that probable cause in such cases was difficult to establish and, two, they did not want to divulge subsequently the existence of the tap.

And therefore, rather than accept those two problems under title III, they just did not engage in any activity at all in the third field of domestic intelligence. Do you have any comment on that? Do you think that is, in fact, their policy?

Mr. BENDER. Well, I think that their second problem, the problem with nondivulgence, is not a particularly real one because when they prosecute they have to divulge anyhow unless the surveillance be legal. And after the *Keith* case it is not legal. And I would urge that the suggestion that Mr. Justice Powell that the Congress enact legislation following the *Keith* case will have to be very carefully reconsidered in the light of the gross misrepresentations as to what intelligence surveillance is in the underlying record in that case.

And I have no hesitancy to tell you that we, as the lawyers in the *Keith* case, will pursue that issue as vigorously as we know how.

Now, as to the probable cause standard, as I understand the fourth amendment, if there is no probable cause, there should not be any surveillance. If there is no probable cause that a crime is about to be committed then there should not be a wiretap unless there can be found a constitutional area where a different standard of probable cause for investigatory surveillance may exist.

Given our recent history with that second kind of probable cause, and I have tried to suggest it is a ruse, I am highly skeptical that such a new standard of probable cause by this Congress or the court could ever be found and I would not want to see any such exception to title III or any other legislation which provides for surveillance on a lesser showing than a showing that a crime is about to be or is being committed under the ruse of investigatory surveillance. I think it would be a terrible mistake and an uncontrollable practice.

As to the suggestion that there has been no surveillance following district court, I would point this committee toward the hearings undertaken in Minneapolis or was it St. Paul, within the last several weeks arising out of Wounded Knee, where they are now about 5,000 pages of court transcript demonstrating an effort by the FBI to wiretap the Wounded Knee participants during the negotiations that took place in the Wounded Knee enclave. And the court has determined that those surveillances were illegal and has ordered they be suppressed, and not be used in the ensuing prosecution.

I know of no other examples by the way but I do know of that one and the committee may want to inquire into it specifically.

Mr. KASTENMEIER. I have many other questions I would like to ask of you, and perhaps we can continue our dialog at another time. These are only the opening hearings on the subject of wiretapping and electronic surveillance. We are not really prepared to consider legislation wthout at least another set of hearings which will be more refined based on these 3 days which have been largely to inform ourselves of the question and try to understand its dimensions. In any event I would like now to yield to my colleague from New York, Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman. Thank you Mr. Bender, for giving us a very interesting statement from the background of your extensive experience with this problem.

I take it you feel, and I think you said, that you do not feel there should be any domestic intelligence surveillance.

Mr. BENDER. That is correct.

Mr. SMITH. Of course if there is no domestic intelligence surveillance the big problem comes, of course, in squaring that with the constitutional guarantee of privacy. And here, of course, you come into the old argument and the ongoing argument of the right of the individual as against the ultimate welfare of the Nation, if anybody can ever make decisions in that regard.

For instance, the problem that we have, the problem that the Congress would have, the problem the people of the country would have, would be we have always felt in this country that differing opinions were perfectly valid and legal, and that even a change of government, if it be done by the ballot instead of the bullet was legitimate. And that is what this country is about. But, an overthrow of the Government by violent and revolutionary means was not contemplated in the Constitution and the feeling has been, of course, all along that the Government ought to be able to protect itself against that kind of activity. The difficulty is who is to say when there is or might be that kind of activity and when there is activity that is protected by the Constitution. And do you see any means which we could devise to protect the Government of the United States against violent overthrow while preserving the rights of the individual under the Constitution?

Mr. BENDER. The Congress grappled with this problem in enacting title III. And in those circumstances where an act of sabotage or treason or the like is about to or has occurred and there is a probable cause to get a warrant, the Justice Department can apply to the court and get a prior judicial warrant, as the fourth amendment re-

quires, authorizing the search and there is even the emergency provision in title III which allows the Department of Justice to act 48 hours in advance of going before a judge to conduct a surveillance

Now, I find it interesting that the 48-hour emergency provision, at least as I understood Mr. Miller's testimony, and from my own experience in this field, never has been utilized. The Government has rather chosen to go the route of intelligence gathering.

I have difficulties with some aspects of title III as administered. But, assuming its constitutionality, and the courts have found it to be constitutional, it seems to be a much safer way to strike the balance that you are talking about; that is, the balance between privacy and the need for the Government to protect its citizenry.

That is, when crimes are or are about to be committed, you get a warrant, and the separation of powers is fulfilled. A judicial officer stands between the zealous prosecutor and the accused and the rights are protected in the constituitonal fashion. I know of no way to answer your specific question where a grant of power to protect the national security could be made and not abused by virtue of its own weak and sweeping definition. I have hoped that we have learned as a Nation in the last 3 years, the danger where national security has been called out to justify some of the most horrendous abuses I believe, by a wide variety of people.

Mr. SMITH. Well, I tend to agree with you, Mr. Bender, in that I cannot see why a proceeding under title III, for instance, in so-called domestic intelligence cases where crime is about to be committed or has been committed, is as difficult for the FBI as Mr. Miller testified. I can understand that it restricts the intelligence-gathering function, but I tend to agree with you that perhaps this is the only way that you can balance the constitutional guarantees.

Mr. BENDER. I think that you will find in looking at some of the record, to which I have alluded, authorizing investigatory national security surveillances, that there is a large measure of fear of constitutionally protected dissent, a very large measure running through these documents. And it is impossible to separate out the zeal with which that fear has been pursued in authorizing surveillances and the effort to use the criminal process in order to, in some of these cases, chill and deter speech and struggling with this problem. I am glad to hear that you are going to struggle with it a long time. And I would hope that you would look at these documents. I think that the proof of an assertion lies in our own recent history with it, and it is a history that has got to be told where intelligence-gathering surveillance has not been used in the way in which it has been justified. It has been used in a highly abusive fashion, and I do hope you will get a chance to look at it and make your own judgment instead of relying on mine.

Mr. SMITH. Thank you.

Mr. KASTENMEIER. The gentleman from Maine, Mr. Cohen.

Mr. COHEN. Thank you, Mr. Chairman. I just have one question.

On page 7 of your statement, Mr. Bender, toward the bottom of the page you say "Upon inspection, defendants were able to determine that a number of these unidentified overhearings were of the defendants themselves, and at least eight were of their attorneys."

How did you make that determination? Do you know of your own knowledge?

Mr. BENDER. Yes. Because the logs gave the phone numbers and it gave the familiar names that the individuals involved used in conversations with their clients. One entry would be "Skip, last name unknown" and then the name of the defendant, and the time and the date and the phone number.

Well, Skip happens to be the name of the attorney whose first name—that was his nickname, and the phone number was his office telephone, so except for the recording purposes, the Government did not make the identification, which by the way, on its face, was patently absurd because the attorney happened to be rather well known in the local georgraphical area, and his nickname appeared in the press frequently and the phone number was certainly well known, and it appeared throughout the logs in question, so it was an obvious abuse.

Mr. COHEN. Well, we had testimony earlier this morning, and I do not know if you were present or not, that whenever an attorney would be talking with his client, that the FBI agent would disconnect, or not monitor that conversation. That seems to be in contrast to your testimony.

Mr. BENDER. I am familiar on this issue with a memorandum from the then Attorney General Mitchell instructing agents to do just that, to interrupt, but we just made available to the seventh circuit, which is considering the *Dellinger* contempt case, some of the documents we found in the *Dellinger* v. *Mitchell*, the civil case, with permission of the district judge here and although I cannot tell you the exact words in the document, in the public brief we filed we suggested that the directive was not followed and we cited to a specific memorandum where a particular conversation between a client and his lawyer discussing trial strategy was mentioned, with a warning at the bottom to be more careful in the future.

Mr. COHEN. Were the Attorney General's guidelines and recommendations limited to the attorney-client privilege, or did they include the doctor-patient, priest-penitent privileges? Do they have any of the other normally recognized privileges?

Mr. BENDER. The one that I have seen, which I believe is dated July 1969, I am sorry, I guess it is July 1970 and I can make that available to the committee if you like——

Mr. COHEN. If you would, yes.

[The document referred to follows.]

JULY 14, 1969.

EXCISED COPY OF MEMORANDUM OF JOHN MITCHELL FURNISHED TO THE DISTRICT COURT BY MR. CALHOUN

J. Edgar Hoover, Director, Federal Bureau of Investigation, and John N. Mitchell, Attorney General

ELECTRONIC SURVEILLANCES

Both the Criminal and Internal Security Divisions have been reviewing the legal problems in connection with present and future prosecutions, in view of the information furnished by you concerning overhearings of some conversations in recent months of some of the defendants involved in the Chicago anti-riot case.

The likelihood of continued interception of several of the Chicago defendants on existing installations does indeed present the possibility of serious legal problems arising in connection with future criminal trials, particularly if a defendant in a pending Federal case is overhead discussing trial strategy or tactics with his attorney. Moreover we must also be aware of the problems presented by an agent of the government surreptitiously overhearing conversations of a defendant which may be relevant to the criminal case. See *Massiah* v. *United States*, 377 U.S. 201.

In an effort to minimize the possibility of overhearing conversations involving defendants or their attorneys which relate to trial strategy I have concluded that the Bureau should undertake the following precautions.

The telephone surveillances which I have authorized should continue under the current directives. However, the Bureau should take steps to insure that each telephone surveillance on should be personally monitored by a special agent or special employee. Each such monitoring agent or employee should be instructed in writing that he is to immediately cease monitoring, both in person and by electronic recording, and conversation as soon as he becomes aware that one of the parties to the conversation is a defendant in a pending Federal criminal case or an attorney of such defendant. For the time being each such agent or employee should be furnished with a list of defendants and their attorneys who are involved in the Chicago anti-riot case so that he will be aware of the persons whose conversations should not be monitored. A list of those defendants and attorneys is attached. He should also be instructed to make a notation in the log, as appropriate, that the conversation was cut off and was not overheard, after identifying the name of the defendant or attorney who was on the line which occasioned the cut-off.

The same procedure should be followed with respect to the monitoring of since it appears that some of the Chicago defendants will be overheard in connection with some of those surveillances. It is also possible that one or more of the defendants or attorneys would be overheard on other currently operative electronic surveillances. Reasonable precautions should be taken to prevent such overhearings. The primary purpose of these procedures is to avoid the government's learning of defense strategy or plans in such a way as there might be an intrusion into the Sixth Amendment rights of a defendant. Any time a conversation relating to such strategy or tactics, between any two persons, takes place, the conversation should be immediately cut off as soon as the subject matter of the conversation becomes apparent.

If a conversation of a defendant or one of his attorneys should inadvertently be overheard and later comes to the attention of a special agent, that special agent shall immediately seal the record of the conversation, attaching a memorandum certifying that he has not and will not orally or in writing relate the substance of the conversation to any other representative of the government or to anyone else except upon order from the Attorney General. This sealed log and the agent's certification should be immediately forwarded to you for transmittal to the appropriate Assistant Attorney General.

I know that these procedures will place an additional burden on the Bureau but I am sure you will appreciate that it is a reasonable balance in an effort to secure needed intelligence and at the same time safeguard future prosecutive steps which should be taken.

Attachment.

Defendants and Attorneys in *United States* v. *Dellinger, et al., N.D. Ill., 69 CR. 180.*

DEFENDANTS

David T. Dellinger
Rennard C. Davis
Thomas E. Hayden
Abbott H. Hoffman
Jerry C. Rubin
Lee Weiner
John R. Froines
Bobby Seale

ATTORNEYS

Charles R. Garry
Michael J. Kennedy
William M. Kunstler
Gerald B. Lefcourt
Dennis J. Roberts
Michael E. Tiger
Leonard I. Weinglass
Stanley A. Bass
Irving Birnbaum
Howard Moore, Jr.

Mr. BENDER. It refers only to the attorney-client overhearings and does not recognize any other privileges.

Mr. KASTENMEIER. That would be very helpful to the committee and we would appreciate receiving a copy.

Mr. SMITH. If the gentleman will yield, I think that Mr. Miller testified this morning that the Attorney General's instructions covered all privileges.

Mr. COHEN. It would be helpful if we can have that.

Mr. BENDER. I will let the memo speak for itself. It is my recollection that only the attorney-client privilege is specifically mentioned.

Mr. COHEN. That is all I have.

Mr. KASTENMEIER. On behalf of our committee, we want to express our appreciation to you, Professor Bender, for your appearance here today.

[The statement of William J. Bender follows:]

PREPARED STATEMENT OF WILLIAM J. BENDER, ADMINISTRATIVE DIRECTOR, CONSTITUTIONAL LITIGATION CLINIC, RUTGERS UNIVERSITY SCHOOL OF LAW, NEWARK, N.J.

Chairman Kastenmeier and members of the subcommittee: I welcome the opportunity to appear before you today and to relate some of my experiences with electronic surveillance matters in several cases, both civil and criminal, in which I have appeared as counsel. The cases include the following: *United States* v. *Ahmad, et al.*, No. 14950, United States District Court, Middle District of Pennsylvania, reported 347 F.Supp. 912 (1972); *United States* v. *Ayers, et al.*, No. 48104, United States District Court, Eastern District of Michigan, Southern Division; *In Re Dellinger, et al.*, 72 Criminal 925, United States District Court, Northern District of Illinois, Eastern Division and the Seventh Circuit Court of Appeals; *United States* v. *Butenko*, United States District Court, District of New Jersey, No. 418–63; *United States* v. *United States District Court*, 407 U.S. 297 (1972); *Dellinger, et al.* v. *Mitchell, et al.*, United States District Court, District of Columbia, No. 1768–69; *Sinclair, et al.*, v. *Kleindienst, et al.*, United States District Court, District of Columbia, No. 610–73; *McAlister, et al.*, v. *Kleindienst, et al.*, United States District Court, Eastern District of Pennsylvania, No. 72–1977. I shall attempt to create a composite picture for you of the governmental abuses of First and Fourth Amendment and statutory Rights from the public records of wiretap matters in these cases. Based on these experiences, I urge you to reject legislation which provides for so-called national security investigatory electronic surveillance of any kind in both foreign and domestic concerns. I will leave the debate on the constitutionality of prosecutorial surveillance authorized by prior judicial warrant to others. However, I will suggest that if the privacy guarantees of the Fourth Amendment are to be meaningful, the Congress must legislate meaningful administrative controls for the conduct of such prosecutorial surveillance. These controls must be implemented vigorously by the legislative branch.

Probably the most serious revelation in these cases has been the discovery that the government intentionally sought to mislead the federal courts into believing that national security electronic surveillance was for investigatory, intelligence gathering purposes as contrasted with prosecutorial electronic surveillance which is utilized to gather evidence. Assistant Attorney General Robert Mardian expressed this proposition in briefs and arguments throughout the *Keith* case:

"This gathering of information is not undertaken for prosecution of criminal acts, but rather to obtain the intelligence data deemed essential to protect the national security." (Government's Brief, at 16)

"We stress once again that, in conducting such national security surveillances, the Attorney-General is gathering intelligence information for the President, not obtaining evidence for use in criminal prosecution." (*Id.*, at 19)

"Moreover, unlike the traditional searches made pursuant to warrant that magistrates issue upon a showing of probable cause, national security surveillances are not designed to obtain facts needed in a criminal investigation, but to obtain intelligence information." (*Id.*, at 25)

"The individual overheard is not himself the subject of surveillance, but his conversation is intercepted incidentally and wholly irrelevantly (in respect to his prosecution), in connection with a surveillance to obtain intelligence information to protect the national security." (*Id.*, at 39–40)

"In this case, the defendant, Plamondon, was not the subject of the surveillance authorized by the Attorney General. He was overheard when, fortuitously, he made a call to the telephone installation which was the subject of the surveillance." (*Id.*, at fn. 18, 40)

At oral argument before the Supreme Court, Assistant Attorney General Mardian again asserted that the case was *not* one, "where electronic surveillance was authorized for the purpose of obtaining prosecutive evidence in a criminal proceeding" or a case "where the defendant was the target of the electronic surveillance which was authorized." (Transcript of Oral Argument at 8) Mardian went on to say:

"And I think that beyond question the in camera exhibit will show that the purpose of the surveillance was for the sole and limited purpose of obtaining counter-intelligence information as distinguished from prosecutive evidence in a criminal case." (*Id.*, at 24)

"In the *Alderman* case, . . . the surveillance was authorized for the purpose of obtaining prosecutive evidence to be used in a criminal case, and it was directed against the defendant. . . . In this case we have a situation, as in *Clay*, where, as I said, the defendant unfortuitiously—or fortuitiously, depending on the outcome of this case—happened to call the wrong number." (*Id.*, at 25)

"The only purpose is, as I have stated: one, to obtain the on-going intelligence necessary to compete in the area of foreign affairs, and the on-going intelligence necessary for this nation to protect itself against not only its foreign foes but its domestic foes." (*Id.*, at 79)

This argument was universally made in all the cases, both foreign and domestic, where the Nixon administration chose to admit to electronic surveillance in recent criminal cases and submit the legality claim to the test in litigation. For example, before the trial the government in *Ahmad*, "admitted to what . . . [it] believe[d] are probably conversations of Sister Elizabeth McAlister, one of the defendants in this case," and conversations having been overheard in a "national" security electronic surveillance authorized by the Attorney General of the United States. (Hearing of May 24, 1971, pp. 56–57.) The government steadfastly maintained from the outset that the overhearing of Sister McAlister was inadvertant, having nothing to do with furthering the prosecution of its case and having no relationship to trial evidence. (T.78).

The government's earlier representations, that whatever illegal electronic surveillance (of the so-called "national security" variety) it may have conducted was only for intelligence data gathering, were promptly contradicted. F.B.I. Agent Smith, who initiated the request for the surveillance in question (Hearing of May 2, 1972, partial transcript p. 31), and then supervised the surveillance operation (T.36), testified in direct opposition to the prior representations of the government attorneys; the surveillance was conducted to gather evidence to further the prosecution in this case (T.24, 45, 47).

In its answer to the motion seeking disclosure of electronic surveillance filed to the indictment, in the *Ayers* case, the government characterized its illegal electronic surveillance activities as they affect this case as follows:

"A review of the records of the Department of Justice has established that the defendants Linda Evans, Dianne Donghi, Russell Neufeld, Jane Spielman, Robert Burlingham were never the subjects of direct electronic surveillance, nor were any premises in which they had a proprietary interest. However, the said defendants did participate in conversations that are unrelated to this case and which were overheard by the Federal Government during the course of electronic surveillance expressly authorized by the President acting through the Attorney General."

An examination of the disclosed logs demonstrated that this statement was patently false. This tap was directed at the national office of an organization of which these defendants were members at a time when the government alleged these defendants, the subjects of the tap, were formulating the conspiracy for which they were indicted. They, contrary to the assertion above, "were . . . the subjects of direct electronic surveillance," and the tap was on the phones of an organization wherein they had constitutionally protected expectation of privacy.

These facts and like circumstances in other cases have been pieced together bit by bit in criminal cases. The conclusion—that the claim of a "fortuitous overhearing" on an intelligence tap was a deliberate falsehood, designed by this administration to hoodwink the judiciary into granting the national security exception to the Fourth Amendment—is borne out by recent events. Civil Discovery, after almost five years of litigation in the *Dellinger* case, has resulted in the disclosure of documentation which pierces the fraudulent claim of intelligence electronic surveillance once and for all. A protective order prohibits the revelation of specifics to this Committee. However, I strongly urge that before any legislation is reported out for floor action, that this Committee seek out from the Justice Department the requests for national security electronic surveillances and the authorizations allowing them. This documentation will demonstrate the extent of the abuses and the need for corrective action.

Interim disclosures by the government in the *Ayers* case reveal the enormity of some of these problems and the difficulty of getting at the truth in the context of a criminal prosecution suppression proceeding.

United States v. *Ayers*, No. 48104, United States District Court, Eastern District of Michigan, Southern Division, was a conspiracy prosecution of the Weathermen faction of the Students for a Democratic Society; the case was dismissed by the Court on October 15, 1973.

The government moved to dismiss this case because of its unwillingness to suffer the revelation of the identity in adversary hearings ordered by the court of an agency that had conducted some of the illegal surveillance activities.

Pursuant to an interim order on June 4, 1973 by the Honorable Damon J. Keith for disclosure of illegal electronic surveillance, the government turned over to the defendants 3,000 pages of transcripts of telephone conversations covering eight months of surveillance. The government asserted that these transcripts represented full compliance with the interim disclosure. Although the judge reserved decision as to whether or not the defendants had standing to receive summary logs of the overhearings made during this time period, twelve days of logs were inadvertently included with the 3,000 pages of transcripts. An inspection of these logs by the defendants indicated that the government was either unwilling or unable to comply with the interim disclosure order concerning surveillance even where illegality and standing were conceded. The logs listed 500 overhearings during the twelve day period; in the 500 overhearings 239 parties were listed as "unidentified" by the government. Upon inspection, defendants were able to determine that a number of these unidentified overhearings were of the defendants themselves and at least eight were of their attorneys. In each of these instances, no transcripts of the illegal overhearings were provided by the government to the defendants.

Simple arithmetic shows the enormity of the problem if the tap operated for eight months at the same level. More than 12,000 overhearings with more than 5,000 unidentified voices occurred.

I don't believe the disclosure failures in virtually all national security electronic surveillance cases are mere happenstance. The indexing and reporting systems within the Department of Justice function so as to avoid rather than allow requisite disclosures in the ciriminal process: In the *Ahmad* case F.B.I. Agent Gary Owen Watt, a supervisor of the F.B.I.'s domestic intelligence division, supervised the general search of records (T.54), pursuant to a letter from the Justice Department attorneys (T.57), in order to disclose any electronic surveillance as to defendants, their attorneys or any unindicted coconspirators. The means for ascertaining the existence of surveillance is an F.B.I. index comprised of an alphabetical list of names (T.57). Index cards would indicate that a telephone belonging to the person listed, was tapped, that someone was overheard who called into the installation, "the date the installation was installed might be also included in the file, and the location . . . possibly" (T.58). Unidentified callers who may only use first names who call into a tapped installation would not be reflected in the index (T.59). Agent Watt was not certain if the fact of the existence of unidentified callers on the tap would be listed in some manner. No index is kept by investigating subject, by name of case or by place. The only way to determine whether someone has been overheard is to search for a name alphabetically in an index file (T.61). Watt knew of no other method within the department of determining whether or not a particular individual has been overheard (T.61–62). The only way to determine if a residence had been overheard would be if the resi-

dence was identified with a name in the index (T.65). The defendants' submission to the government of a list of places, wherein they had an expectation of privacy, to assist the government in searching its files, was a worthless exercise because, "if his name wasn't mentioned, his name wouldn't be included in the indexes [sic]" (T.67). Where several people shared a residence with a tapped phone, only the name of the telephone subscriber would appear on the index, not the other users of the phone. No search was made for an item "Religious Sacred Heart of Mary," the residence of Defendant Sister McAlister, one of the places listed in defendants' motion (T.77).

In the *Ahmad* or Harrisburg conspiracy case the tentative determination of the participation of Sister McAlister on the calls was surmised by the government by reference to the telephone numbers that were called by the subject of the surveillance (T.12), namely the number of the convent where Sister McAlister then resided along with other nuns. However, no effort was made to identify the voice of any person calling into the tapped location during the course of the surveillance or afterward (T.14). Unless a full name was mentioned in the course of a tapped conversation, the only means of identification was by way of the name of the phone service subscriber to whom the intercepted call was made (T.14). F.B.I. Agent Smith recognized that often in phone conversations, a full name is not used, as was the case with the two logs before the court where only a first name, to wit, "Liz" was used (T.15). The agent also recognized the possibility that names are not always used (T.18), making identification by names impossible. The mechanical devices which recorded the phone numbers of out-going calls from the tapped location could not register the phone numbers of incoming calls, so incoming calls were not formally identified for record-keeping purposes.

This is not to suggest that agents' overhearing calls or conversations during the course of an investigation lack the capability of acting on their "tentative" identifications. The problem faced by defendants is that the reality of the government's prosecutive use of electronic surveillance is carefully concealed from judicial scrutiny.

I urge this subcommittee to deeply probe the Justice Department during these deliberations on the following issues:

(1) How are agents of the F.B.I. instructed to circulate facts during an investigation which are gleaned from an electronic surveillance source? Testimony in some cases and recently revealed specific documentation in materials covered by protective orders will show elaborate efforts to conceal electronic surveillance sources. This practice makes a showing of taint extremely difficult and insulates illegal activity from even internal Justice Department controls.

(2) How are electronic surveillances numerically counted and described to the legislative and judicial branches? These materials will show efforts to conceal the extent of national security electronic surveillances by grouping many surveillances under a specific reporting heading.

(3) How has the Justice Department sought to analyze the foreign and/or domestic character of its national security surveillances? These materials will show an attempt to over-emphasize the contacts and involvements with persons in foreign countries by the subjects of certain surveillances to support arguments in court of the foreign security character of the electronic surveillances in question.

(4) How extensive has national security surveillance been? Disclosed materials would indicate that the program was far more extensive than anything indicated in Department of Justice statistics.

(5) What are the constitutional consequences of the national security electronic surveillance program? Materials already disclosed indicate a surveillance program of breath-taking enormity involving hundreds of thousands of overhearings, authorized on fear, innuendo and speculation without regard to the privacy rights and rights of association and free speech of a free people. The program is the consequence of raw executive power, unchecked by this legislature or the judiciary. To legislate against and then to control these abuses a full investigation must be undertaken and specific review procedures established.

I close these remarks by asking you whether these past two years, characterized as they were by the constant invocation of the spectre of threats to national security for all necessary occasions will foreclose the meaningful pursuit of your task. I would hope that recent history suffices to demonstrate that

the shop-worn talismanic incantation "national security" can no longer foreclose democratic processes. A good beginning would be full scrutiny of the entire national security electronic surveillance program and the legislation of substantial controls to prevent its ugly reoccurrence.

Mr. KASTENMEIER. With that, the Chair will also announce that statements of Congresswomen Abzug and Mink, Congressman Kemp, and Dr. Lapidus will be accepted for the record and that the record will be kept open for a period of two weeks during which time other relevant material and statements can be received for inclusion therein.

[The statements referred to above follow:]

STATEMENT OF REPRESENTATIVE BELLA S. ABZUG

Mr. Chairman and members of the subcommittee, I appreciate the opportunity of appearing before you today to discuss a subject about which I feel most strongly and to speak in support of two bills which I have introduced to guarantee to individuals their constitutional rights of privacy, H.R. 9698 and H.R. 9815.

The first of these bills would make a simple but significant change in Section 2511(2)(c) and (d) of Title 18 of the United States Code. It would provide that wire and oral communications can be intercepted without a judicial warrant only if all the parties to the communication give prior consent. The second bill, H.R. 9815, would prohibit investigations, surveillance, or data-keeping by the military into the beliefs, associations or political activities of civilians and civilian organizations.

For many years, I and several of my colleagues in both bodies of Congress have spoken out in decrying the violations of privacy and other individual rights perpetrated by the government in the guise of its legitimate functions. But our voices seemed to fall on deaf ears. Now, however, the protection of privacy has become a more popular issue and even a "fashionable" legislative subject. In this session of Congress alone, more than a hundred different bills and resolutions relating to privacy have been introduced and are now being considered by several committees of the House. A recent Harris Poll indicated that the general public, by 77 per cent to 14 per cent, overwhelmingly favors passage of legislation to curb the abuses of governmental wiretapping and bugging. And last February even President Nixon, in creating his Committee on the Right of Privacy, headed by Vice President Ford, recognized the dangers to our democratic institutions that invasions of privacy represent. Perhaps it took the shocking disclosures of the Watergate scandals to awaken the general public and my colleagues to the realities of life in this electronic age and to the urgent need for legislation to place some limitations on unbridled government snooping. Whatever the causes for the change in attitudes, I am delighted that it has come about, that the time is now ripe for passage of legislation that will put an end to ever-increasing governmental intrusions on citizens' private lives. The hearings which this subcommittee is now conducting give me hope that we may still be able to check, before it is too late, the drift towards totalitarianism and thought control which must ensue when every aspect of an individual's life is subject to electronic monitoring.

These words may sound overly dramatic but there is no more insidious invasion of privacy than electronic surveillance. It is insidious not only because of its covert nature—even now this subcommittee does not know how many warrantless wiretaps were approved by the Department of Justice in 1973—but because it reaches into the innermost aspects of an individual's life, to his thoughts and beliefs, to those basic rights that are guaranteed by the First Amendment. As Ramsey Clark stated when, as Attorney General, he testified in support of the Right of Privacy Act of 1967 (S. 928):

"Nothing so mocks privacy as the wiretap and electronic surveillance. They are incompatible with a free society and justified only when that society must protect itself from those who seek to destroy it."

I agree wholeheartedly.

The use of wiretapping and electronic surveillance is relatively recent, dating only from the invention of the telephone. With the increasing sophistication of electronic devices, undoubtedly the use of such devices has kept pace

with their refinements though none of us can claim to know the real extent of this use. Aside from Congress' need to know the extent of warrantless wiretaps *authorized* by the Department of Justice, we have no idea of the degree to which *unauthorized* wiretapping has been engaged in by Federal agents or to what extent other types of electronic surveillance have been employed. Without this knowledge, we cannot begin to measure the value or necessity of electronic monitoring in the area of crime control or national security.

Since the invention of the telephone, the microphone, and recording devices, the courts and the Congress have been attempting to reconcile this necessity with the fundamental constitutional rights guaranteed by the First, Fourth and Fifth Amendments. The issue of the use in a criminal trial of evidence obtained by wiretapping first came before the U.S. Supreme Court in 1928, in *Olmstead v. United States*, 277 U.S. 438 (1928). On a five to four vote, the Court held that wiretapping was not within the confines of the Fourth Amendment, interpreting the search and seizure proscription as applying only to physical property and tangible items. In a vigorous dissent, Mr. Justice Brandeis stated:

"To protect [the right to be left alone], 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 . . . There is, in essence, no difference between the sealed letter and the private telephone message . . . The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded and all conversations between them upon any subject . . . may be overheard."

Six years later, Congress enacted the Federal Communications Act of 1934, 48 Stat. 1103, Section 605 of which provided that ". . . no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, purport, effect, or meaning of such intercepted communication to any person." Unfortunately, no well-established consistent body of case law developed in the years that followed. The leading Supreme Court cases, before the enactment of the Omnibus Crime Control and Safe Streets Act of 1968, were *Berger* v. *New York*, 388 U.S. 41 (1967), and *Katz* v. *United States*, 389 U.S. 347 (1967), in which the Supreme Court in essence adopted Justice Brandeis' dissent in the *Olmstead* case, and held that electronic eavesdropping was subject to the requirements of the Fourth Amendment. Mr. Justice Stewart, speaking for the Court in the *Katz* case, (389 U.S. at 352-353) stated:

"We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling. The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied . . . and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."

In 1968, following the *Berger* and *Katz* cases, Congress attempted to resolve the dilemma by enactment of the Omnibus Crime Control and Safe Streets Act. This, as you no doubt recall, was during a period when "crime in the streets" was becoming a major political issue and crime control was more popular than the protection of privacy. Although certain types of wiretapping and electronic eavesdropping were prohibited and criminal sanctions and civil remedies were provided, Congress for the first time, in Title III, specifically authorized the use of electronic surveillance in criminal investigations and specifically exempted national security cases from any of the restrictive provisions of the Act. Here again those two familiar catch-alls—criminal investigations and national security—were used to justify governmental invasions of privacy.

One of my bills, H.R. 9698, which is identical to H.R. 9667, introduced by Rep. Long and co-sponsored by twenty five other Members of the House, would amend 18 U.S.C. Section 2511 (2)(c) and (d) by providing that wire and oral communications can be intercepted lawfully without a judicial warrant only if all the parties to the communication give prior consent. The present Act requires the consent of only one party to the communication. The Department of Justice is opposed to this bill as it is to all proposed amendments to Title III. First, the Justice Department argues, its "successes require (them) to recommend that Title III remain unchanged." Electronic surveillance techniques have allegedly been most effective, if not indispensable, in combatting organized crime. As the Justice Department has yet to furnish any concrete

evidence in support of this allegation. I have no way of knowing how valuable—necessary—electronic surveillance has been in controlling crime.

Second, the Justice Department argues, HR 9698 would negate any efforts to obtain evidence by investigative procedures that have consistently been approved by the Supreme Court. It is true that the Court has drawn a distinction between electronic surveillance without the consent of any of the parties, requiring a court order and a showing of probable cause, and the monitoring of conversations with the consent of only one party. As recently as *United States* v. *White*, 401 U.S. 745 (1971), a closely divided Supreme Court adhered to its old ruling that the use of bugged informers was outside the requirements of the Fourth Amendment. The railroads appear to be that one who confides—or talks to—another assumes the risk that his confidence may be disclosed and the risk is no different even if the other person is recording or broadcasting the first person's disclosures. I submit that these cases are bad law. The number of separate opinions in the *White* case and the lack of a majority opinion are evidence of the lack of consensus in this area. Moreover, if existing law permits the interception of communications without a warrant or any showing of probable cause or even of reasonableness without the prior consent of all the parties to the communication—and the *White* case and Section 2511 (2)(c) and (d) so indicate—there is a clear need for a change in the law. The Federal Communications Commission, in instituting the "beep tone rule" and in prohibiting eavesdropping by radio devices unless all parties to the communication consent, has already recognized this need. The FCC regulations, however, lack effective sanctions—only discontinuation of telephone service or a $500 fine. My bill, however, would make willful interception, disclosure, or use of a wire or oral communication without the prior consent of all parties subject to the existing criminal penalties and civil remedies provided in Title III. As the existing provisions for court ordered interceptions in criminal investigations would still be available, it can hardly be argued—as both the Justice and Defense Departments do—that the amendment proposed by HR 9698 would seriously hamper crime control activities.

Although HR 9698 would amend only one section of Title III, increasing the types of cases in which a judicial warrant would be required, there are other bills presently before this subcommittee which would make more sweeping changes. Rep. Drinan's bill, for example, HR 9781, would eliminate all provisions of the Act authorizing electronic surveillance and would retain only those sections prohibiting the interception, use, or disclosure of any wire or oral communication without the prior consent of all parties to the communication. H.R. 13825, introduced by the Chairman of this subcommittee and identical to a bill introduced by Senator Nelson, would provide specific controls for the use of electronic surveillance in "national security" cases. Following guidelines suggested by the Supreme Court in the *Keith* case (*United States* v. *United States District Court*, 407 U.S. 297 (1972)), it would prohibit all warrantless wire or oral interceptions (except for one party consensual interceptions and others enumerated in Section 2511 (2)), but would require less than a showing of "probable cause" to obtain a judicial warrant to authorize surveillance of a foreign power or its agents.

Because of my own opposition to Title III of the Omnibus Crime Control and Safe Streets Act, I am convinced that more basic changes are needed than those proposed in my bill. In the area of criminal investigation, for example, the standards set forth in Section 2518, even if strictly adhered to—as the Justice Department so painstakingly asserts has been done—are hardly adequate to meet the test of "narrowly circumscribed" surveillance required by the *Berger* and *Katz* cases. Perhaps electronic surveillance, by its very nature, can never conform to the strict requirements of the Fourth Amendment, even when such surveillance is conducted pursuant to a judicial warrant. As the ACLU has pointed out in its excellent presentation before this subcommittee, "the technology itself stands in the way of any kind of effective control."

It is certainly arguable that even court authorized electronic surveillance, as conducted under Title III, may be proscribed by the Fourth Amendment. There is no doubt, however, that warrantless wiretaps and monitoring conducted by the government in the guise of "national security" present a clear threat to our basic First Amendment rights. Because of the imprimatur of "security," these activities are shielded by a veil of secrecy not only from the individuals subjected to surveillance but from the courts and the Congress as well. And, unless they are known, they cannot be subject to challenge or to

control. It is only in recent years that we have begun to learn of government spying and snooping dating back to the sixties. We may never learn the full extent of this activity. More recently, we have heard sordid accounts of incidents occuring during this Administration—spying activities, wiretapping, and other forms of surveillance directed at law abiding citizens suspected only of engaging in political dissent or viewed as political "enemies"—all undertaken by the federal government in the name of "national security."

A 1971 Senate subcommittee report revealed, for example, that during the late 1960's extensive spying was secretly conducted by 1500 agents of the Defense Intelligence Agency on more than 100,000 civilians. Anti-war activists, blacks, and students were particular targets. After disclosure of this illegal political surveillance in 1971, the Pentagon issued strict regulations against spying on civilians. Yet a Senate committee recently learned that the U.S. Army has continued to maintain numerous surveillance operations on civilians in the United States.

The Department of Defense, in its testimony before this subcommittee, unequivocally stated that it does *not* conduct electronic surveillance of civilians not affiliated with the Department. It cited DOD Directive 5200.27, which expressly forbids such practices "except in narrowly defined circumstances." It did not, however, explain the nature of those circumstances.

The DOD testimony indicated, however, that neither the Omnibus Crime Control Act nor its DOD regulations apply to its activities outside U.S. territory. Its overseas activities, even when directed at United States citizens, are governed by the Status of Forces Agreement and the laws of the host country. There appear to be no constraints on its spying activities, or any explanations deemed necessary for the lack of constraint.

During the 1972 Presidential campaign, army authorities sent intelligence agents to infiltrate a branch of the U.S. Democratic party in Berlin, as well as an offshoot of the American Civil Liberties Union and a group of Protestant missionaries supported by the World Council of Churches. For at least a year, these agents photographed members, acquired lists, opened mail, copied correspondence, and reported on the activities of the Berlin Democratic Club and Concerned Americans in Berlin. An autographed copy of a photograph of George McGovern was solemny regarded as a suspicious document and duly noted. The agents' attempt, apparently, was to link the Berlin Democrats to so-called leftist groups in America and to the East German communists . . . just as McGovern supporters in this country were harassed and put on "enemy lists."

Although the United States Army sought to justify the surveillance of these American civilians on "national security" grounds—that is, they were responsible for "dissidence" among American troops—nothing even remotely subversive was ever discovered and no action was taken against any of these civilians. But the danger lies in the fact that these military agents collected reams of data on the personal lives and politics of American citizens and delivered them to an undercover army "countersubversive" intelligence unit. Reports were then forwarded to the chief intelligence officer in Europe who was later promoted to a top intelligence job in Washington.

Senator Lowell Weicker turned the documentation of this spying over to the Senate Armed Services Committee, but very little happened. The Army explained that such spying was legal in Germany. West German officials even cooperated by tapping telephones themselves. Further, they said, it was not political in nature—though no one seems to have been keeping records on any chapters of CREEP in Europe.

It is hardly necessary to comment on the intimidation that results from this kind of snooping. Were it allowed to continue unchecked, the democratic process would wither away. Fortunately, vigilant citizens and concerned members of Congress will not allow this to happen.

My bill, H.R. 9815, which is identical to a bill introduced in the other body by Senator Ervin, is specifically directed at this kind of unconstitutional surveillance. The bill would prohibit use of the Armed Forces or of any State militia to conduct investigations into, maintain surveillance over, or record or maintain information regarding the beliefs, associations or political activities of any civilians or civilian organizations. The bill provides criminal penalties for civil or military officers who violate these provisions and also provides civil remedies for damages and for injunctive relief.

It is clear that there is a real need for legislation in this area. U.S. citizens, only because they are situated abroad, are being denied their constitutional rights, not by any foreign nation but by an arm of the U.S. government. This the DOD has admitted. With respect to Defense Department activities in this country, it should be clear by now that we can no longer rely on the military to observe its own regulations. I urge you to give favorable consideration to this bill, not onl to rectify the situation in the Defense Department, but to guarantee to all U.S. citizens their First Amendment rights.

TESTIMONY OF REPRESENTATIVE PATSY T. MINK

Chairman Kastenmeier and distinguished members of the Subcommittee, I appreciate this opportunity to speak in support of legislation to protect our citizens' right to privacy.

I am a co-sponsor of H.R. 9973, the principal sponsor of which is Congressman Long of Maryland. This legislation is the same as his own bill, H.R. 9667, and is one of those being taken up in these hearings.

The purpose of this bill is to require the consent of all persons whose communications are intercepted under certain provisions relating to types of eavesdropping. Specifically, it would amend Title 18 of the United States Code to provide "It shall not be unlawful under this chapter for a person to electronically record or otherwise intercept a wire or oral communication where all parties to the communication have given prior consent to such interception unless such communication . . . (was) for the purpose of committing any criminal or tortious act . . ."

We are seeking to forbid any taping or other listening-in on conversations until all parties involved have been informed of it. Courts would still have the power to authorize wiretaps for investigations of criminal activities or because of urgent national security needs.

The need for this change was made clear by the disclosure of the White House taping system, in which recordings were made of Government officials, members of Congress, foreign diplomats, and White House staff members without their knowledge or consent.

Unfortunately, the development of our laws as construed by various court rulings is that it is now perfectly legal to tape record the conversation of someone else as long as *one* party knows of and consents to such recording. In other words, I might call another person on the telephone, tape our conversation, and use it for my own purposes and use it without fear of violating the law.

Obviously, this practice poses grave danger to our historic concept of the Right of Privacy. Every American assumes he has a legal, constitutional right to a certain privacy in his conversations whether in his own home, office, or elsewhere. Yet this is not the case, since the law as construed by courts permits interceptions as I have outlined.

The only way we can restore guaranteed privacy, and at the same time permit criminal investigations where authorized by a court, is to enact this change in our laws. If somebody wished to record a conversation for legitimate, non-criminal purposes, such as to keep a historic record, he would need only so advise the other parties and secure their permission.

I believe this legislation is sorely needed to close a deplorable gap in our laws adversely affecting each American's rights. I urge its adoption by the Subcommittee.

CONGRESS OF THE UNITED STATES,
HOUSE OF REPRESENTATIVES,
Washington, D.C., April 10, 1974.

HON. ROBERT W. KASTENMEIER,
Chairman, Subcommittee on Courts, Civil Liberties, and the Administration of Justice, Committee on the Judiciary, Washington, D.C.

DEAR BOB: First, you are to be congratulated for scheduling public hearings on pending legislation relating to wiretapping and other forms of electronic surveillance. It is a subject on which Congress has not moved for far too long.

I am forwarding herewith a Statement on this subject matter, specifically on my bill, H.R. 11838, to require *prior* court approval on all wiretap and electronic surveillance orders. I would appreciate it if this Statement could be put into the record of your proceedings on the first day of the hearings.

If there is anything which I can do to mobilize colleagues on this matter, please let me know.

Until then, I am,

Sincerely,

JACK KEMP.

STATEMENT OF REPRESENTATIVE JACK KEMP OF NEW YORK

Mr. Chairman, the subject of wiretapping and other forms of electronic surveillance is a matter intertwined with the right to privacy—the right to be let alone, the right to be left alone. It is a right which forms the basis—serves so to speak as the common denominator—of such protections as those shielding the individual against unwarranted searches and seizures, snooping investigations and fishing expeditions by authorities, the inspection of personal papers, records, and effects.

Support for this right runs deeply in the spirit of Anglo-American jurisprudence. As Mr. Justice Brandeis observed in his 1928 opinion in Olmstead against United States, the makers of our Federal Constitution recognized the significance of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of man's spiritual nature—the pain, pleasure and satisfaction of life—is to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions, and their sensitivities. They conferred, over and against the Government itself, a right to be left alone—a right to privacy—the most comprehensive of rights and the right most valued by civilized men. From that awareness arose the adoption of our Bill of Rights, containing the essential protections of the individual, giving to the individual the force of law to say to an agent of the Government, "No, you cannot come into my house or into my life, by any means, without my consent or the full requirements of law and due process."

Certainly, on some issues before this House and the Congress, there must be no retreat from our resolve. The insuring of adequate safeguards to protect the individual's right to privacy, in all its myriad of forms, is such an issue. That is why I am so impressed with the Subcommittee moving at this time towards the consideration of legislation to remedy the shortcomings in present law as to wiretapping and electronic surveillance.

THE PROVISIONS OF H.R. 11838

Mr. Chairman, on December 7, 1973, I introduced the measure H.R. 11838 a bill to amend sections 2516 (1) and (2) of title 18 of the United States Code to assure that all wiretaps and other interceptions of communications which are authorized under those sections have prior court approval. The key here is "prior court approval."

The bill is short in length but long in importance, for the obtaining of court approval as an afterthought when one perceives that evidence gathered might have to be introduced in court on one hand and the obtaining of prior court approval in all instances before information is gathered on the other hand is difference between inadequate protection of rights and more adequate protection. This is, therefore, a crucial distinction.

Why is this legislation desirable?

THERE IS A LOOPHOLE IN THE PRESENT LAW

Chapter 119, Wire Interception and Interception of Oral Communications, of title 18 of the United States Code is the applicable Federal law governing the interception and disclosure of wire and oral communications.

In short, this law prohibits such interceptions and disclosures, except in those specifically defined instances in which the Attorney General of the United States, or any Assistant Attorney General specifically designated for such purpose by him, obtains authority, upon application to a Federal judge

of competent jurisdiction to make an interception. It also authorizes the principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of the State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire or oral communications.

There is a loophole or escape valve built into the present text in each instance, to wit: The language—"an order authorizing or approving" and "when such interception may provide or has provided"—allows a Federal agency or a State or local prosecutor to first intercept, then thereafter get a retroactive approval. Clearly, the language permits retroactive approval of wiretaps and other interceptions. One is left with an impression that these agencies may, in fact, seek a court approval only if they determine that the evidence gathered might be used in court and therefore ought to be safeguarded by an appearance of having been proprietous and in compliance with due process requirements.

I must state for the record that I have no specific knowledge of particular instances of government wiretaps where subsequent approval, after the fact, was obtained. The Department of Justice has not provided the Congress, to the best of my knowledge, with a disclosure on the ratio between interceptions which are done pursuant to a prior court order and those which are approved retroactively. But, it is not unreasonable to assume, since such retroactive approval is customarily sought when the government wishes to proceed in open court with the disclosure of information obtained through the interception, that there might be some instances, perhaps many, where because information is not to be used in open court, the government does not obtain even retroactive approval—no approval at all—thereby failing to meet the requirements of the law. It is, further, interesting to note that the disclosures made by the government on the extent of interceptions during recent years have been couched in terms of court-approved interceptions.

Mr. Chairman, I do not intend to offer testimony today on the more basic subject of whether interceptions should be authorized at all, or under what particular circumstances. My purpose is to draw to the attention of the Subcommittee the loophole in the present law, for surely, irrespective of what else is decided by the members of this Subcommittee and your parent body, this loophole ought to be plugged.

Only when there is prior approval—requiring full prior disclosure to a member of the Bench, giving him thereby an opportunity to refuse to grant such approval if he deems it unwarranted—are the rights of our citizens more adequately protected against intrusion and interference by government. The history of the Bench and Bar in our country shows clearly that certain restraints flow naturally from an awareness on the part of law enforcement officers that certain procedural requirements must be met in order to successfully conclude an investigation or prosecution. These restraints are one of the most effective guarantees of the rights and liberties of our people, collectively and as individuals.

I respectfully request the Subcommittee to act favorably upon the provisions of the bill which I have introduced. I am aware that its provisions may well be incorporated wholly in a bill of larger scope; that is understandable and it may be desirable. But the point is clear: We must tighten this loophole.

STATEMENT OF DR. EDITH J. LAPIDUS, PROFESSOR OF CONSTITUTIONAL LAW AT QUEENS COLLEGE OF THE CITY UNIVERSITY OF NEW YORK

Mr. Chairman, members of the Committee: My name is Edith J. Lapidus. I am a member of the New York Bar and am admitted to practice before the United States Supreme Court. I teach Constitutional Law at Queens College of the City University of New York and hold a Ph.D. degree in Political Science from the City University. My book, "Eavesdropping on Trial," with a Foreword by Senator Sam J. Ervin Jr., was released by Hayden Book Company Inc. of Rochelle Park, New Jersey, in January 1974. It presents an analysis and evaluation of the law and practice under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 in which Congress, for the first time in the history of the United States, sanctioned wiretapping and electronic surveillance by government officials.

I deeply appreciate this opportunity to appear before you and to discuss the problems associated with government eavesdropping and the conflict that it raises between the individual's right to privacy and society's need for effective law enforcement in dealing with crime. This complex and controversial subject has suffered in the past from ideological and political partisanship, and (at least before "Watergate") from public indifference. In my study of wiretapping and electronic surveillance under Title III of the 1968 Act, I have tried to be as objective, unbiased, and impartial as possible, and to offer some constructive and realistic proposals.

This Statement is based largely on my findings as reported in "Eavesdropping on Trial", but it also includes proposals suggested by events that have occurred since the book went to press and further reflection. Problems of *court-ordered* wiretapping and electronic surveillance by law enforcement officials are emphasized in this Statement and discussed in detail. Criticism of *warrantless* eavesdropping, a serious loophole in Title III considered fully in my book, is merely outlined here.

PURPOSES AND PROVISIONS OF TITLE III

Title III is one of eleven "Titles" in the Omnibus Crime Control and Safe Streets Act of 1968, passed by Congress in the wake of a nationwide fear of crime and clamor for "law and order." It purports to serve a dual function:

1. To protect the privacy of individuals by banning *private* eavesdropping, and prohibiting manufacture, sale, possession, or advertising of eavesdropping devices designed primarily for surreptitious interception.

2. To combat organized crime and other serious offenses by giving law enforcement officials an effective tool—interception of wire and oral communications, under specified conditions and with proper safeguards.

The 1968 law is an attempt to balance "liberty" against "law and order." It prohibits interception of wire and oral communications and then makes certain exceptions: designated Federal and State officials are authorized to intercept such communications in the case of specified offenses, provided they comply with procedures detailed in the law. The heart of this procedure is the obtaining of a *court order* from a judge of designated courts, similar to a warrant for search and seizure. In some instances, eavesdropping by law enforcement officials in permitted *without* court order.

COURT-ORDERED EAVESDROPPING

The safeguards to individual privacy sought to be provided by Title III consist of requiring a court order before a government official may intercept a wire or oral communication. A judge is to decide whether or not an order shall be issued, and the interception is subject to supervision by him. Title III lists a wide variety of offenses for which a court order may be obtained, the Federal officers who may apply for a court order, the judges to whom applications must be presented, and the necessary findings by the judge of "probable cause" on which orders are to be based. State officials may also apply for court orders to wiretap or conduct electronic surveillance provided the particular State enacts a law conforming to Title III.

An order may be granted for a period not exceeding thirty days, with an indefinite number of renewals, each for a period up to thirty days. Notice of the interception must be given to the persons named in the order or application, and to others in the discretion of the judge, within ninety days after termination. Judges and prosecuting officials are required to file reports on each order with the Administrative Office of the United States Courts in Washington, D.C., and this agency, in turn, must file an annual report with Congress.

Heavy penalties are provided for violations of Title III: imprisonment up to five years and a fine of $10,000 or both. Civil damages are also recoverable—actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation, or $1,000, whichever is higher; punitive damages and counsel fees and other litigation costs are also recoverable. Conversations intercepted unlawfully are barred from introduction in evidence.

These seemingly simple provisions for court-ordered eavesdropping by government officials have raised some difficult legal and practical questions and generated much heated discussion. They purport to comply with requirements of the United States Supreme Court laid down in two landmark decisions

handed down in 1967, *Berger* v. *New York* (388 U.S. 41) and *Katz* v. *United States* (389 U.S. 347), and law enforcement officials claim that their practices follow the mandates of the Supreme Court. *Berger* struck down as unconstitutional a New York law permitting court-ordered eavesdropping on the ground that the statute was "too broad in its sweep" and failed to provide adequate judicial supervision or protective procedures. In *Katz*, the Supreme Court held for the first time that electronic surveillance constitutes a "search and seizure" subject to the protections and limitations of the Fourth Amendment to the United States Constitution which provides:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Critics of Title III protest that the safeguards sought to be provided by the court order requirements are inadequate; that many terms and clauses in the law are ambiguous; that State and Federal officials are misinterpreting some provisions and failing to carry out others. My study of the law and practice under Title III has led me to the conclusion that there is validity in these criticisms, and I shall discuss them in detail later in this Statement. Even the most ardent proponents of government eavesdropping will admit, I think, that no acceptable balance between liberty and "law and order" can be achieved without clarity in the law, existence and observance by law enforcement officials of proper standards and guidelines, and scrupulous adherence to the safeguards sought to be provided by Title III.

EAVESDROPPING WITHOUT COURT ORDER

In addition to court-ordered eavesdropping, the Federal law permits wiretapping and electronic surveillance by government officials *without* court order in two broad types of cases: (1) during a forty-eight-hour emergency, and (2) to protect "national security" under authority of the President. *Emergency* situations are described as involving two types of conspiratorial activity: 1 Threatening national security, and 2 characteristic of organized crime.

The emergency clause [Sec. 2518 (7)] has been widely attacked as vague, open to abuse, and unconstitutional. The term "national security" is not defined, and the law does not indicate what offenses are "characteristic of organized crime." No report is required to be filed, and there is no way of knowing how much "emergency" eavesdropping has been going on. The law requires that all conditions necessary for issuance of an order under Title III be present before emergency surveillance begins, but it seems unrealistic to assume that these conditions will always be satisfied. The conclusion is compelling that if emergency eavesdropping without court order should be permitted at all, it should be restricted to cases involving a threat to actual or potential attack by a foreign power, collection of foreign intelligence information, or investigation of espionage activity.

In addition to the emergency clause, exemption from court order requirements is provided for national security related eavesdropping undertaken "by authority of the President" [Sec. 2511 (3)]. Title III declares that nothing in the Act shall limit the constitutional power of the President to take measures hat he deems necessary: 1. To protect the Nationa against actual or potential attack or other hostile acts of a foreign power; 2. To obtain foreign intelligence information deemed essential to the security of the United States; or 3. To protect national security information against foreign intelligence activities.

Nor is any limitation to be placed on the constitutional power of the President to protect the United States against: (1) overthrow of the Government by force or other unlawful means, or (2) any other clear and present danger to the structure or existence of the Government. Interception without court order must, however, be "reasonable," if the communications are to be received in evidence in any trial, hearing, or other proceeding.

Warrantless eavesdropping under presidential authority has raised a storm of protest that has not yet fully subsided. Many who were willing to accept court-ordered eavesdropping to combat crime denounced the provision dispensing with judicial sanction as highly ambiguous and unconstitutional. Objections increased in bitterness when the Government claimed that national security

may involve threats from *domestic* groups as well as from foreign powers, and it was revealed that Federal agencies had tapped the telephones of political dissidents without court order. On June 19, 1972, the United States Supreme Court ruled, by a vote of 8 to 0, that presidential authority to protect the nation does not give the Government power to tap without court order the wires of domestic radicals who have "no significant connection with a foreign power, its agents, or agencies" (*United States* v. *District Court*, 407 U.S. 297).

The opinion in the case against the District Court was written by Justice Powell. While the decision was hailed as a victory by civil libertarians, the objections to warrantless eavesdropping in national security cases have by no means subsided, nor are the problems fully resolved. The Government may still claim that some radicals whose phones have been tapped without court do have "a significant connection with a foreign power, its agents, or agencies," thus removing them from Fourth Amendment protection. The decision of the Supreme Court may also have left a loophole by suggesting that traditional warrant requirements were not "necessarily applicable" in domestic security cases.

United States v. *District Court* is a first step in outlawing government eavesdropping without court order in domestic security cases. Warrantless interception circumvents the "probable cause" requirement, and no disclosure to a judge or anyone else need ever be made. There is no way for Congress or the public to know how much eavesdropping is going on if no court order is obtained. "Domestic security" is a vague concept, and it may be difficult to determine if a threat is foreign or domestic without first tapping or bugging. If adequate delineation is impossible, then the warrant procedure should be required in all cases and no "national security" exception to a court order should exist. For a detailed discussion of warrantless eavesdropping in so-called national security cases, see "Eavesdropping on Trial," page 96 et seq. Since publication of the book, I have come to the conclusion that Congress must make it impossible to engage in illegal eavesdropping under the shield of "national security" by requiring a court order in this type of investigation. H.R. 9781 introduced by Mr. Kastenmeier on March 28, 1974 in the House of Representatives appears to effect such a change in Title III by defining a "foreign agent" and requiring a court order in national security cases.

CONSENT EAVESDROPPING

One of the exceptions from court order requirements of Title III is "consent" eavesdropping. Section 2511(2)(c) declares that it is not unlawful for a law enforcement officer to intercept a wire or oral communication if he is a party to the communication or if one of the parties gave prior consent to the interception. This provision of the law was no innovation in policy. If reflected the decisions of the United States Supreme Court which, over a period of two decades, had generally sanctioned eavesdropping without a warrant if one of the parties to the conversation gave his consent to the interception.

Prior to enactment of Title III the leading cases on the subject of consent eavesdropping were *On Lee* v. *United States*, 343 U.S.747 (1953) and *Lopez* v. *United States*, 373 U.S.427 (1963). *On Lee* involved third-party monitoring of conversations; *Lopez* ruled on single-party informant "bugging." In *On Lee*, the Supreme Court upheld the right to wire an informant for sound in order to transmit statements of a suspect to police officers listening at a receiver outside the building. In *Lopez*, a government agent was equipped with a pocket wire recorder which recorded conversations of a cabaret operator offering a bribe to an agent to help him conceal tax liability. The Supreme Court ruled that the evidence and that there was no violation of the Fourth Amendment to the Constitution, although no warrant had been obtained.

The traditional principle on which the validity of consent eavesdropping without a warrant rests is that a party to a conversation takes his chances that the other participant may increase his present or future audience. Justice Brennan, dissenting in *Lopez*, protested that "in a free society people ought not to have to watch their every word so carefully."

Since enactment of Title III, the Supreme Court has help that the Fourth Amendment is not violated by governmental electronic eavesdropping effected by wiring an informant for sound, having him talk to the suspect, and then having agents to whom the conversation is transmitted repeat the communications at the suspect's trial (*United States* v. *White*, 401 U.S.745 (1971)).

Deep cleavages in the Supreme Court on the subject of consent eavesdropping were revealed by the opinions of the Justices in *White*. The Court reversed the judgement of the Court of Appeals and upheld White's conviction by a vote of 6 to 3, but no agreement could be reached on a majority opinion.

The plurality view in *White*, expressed by Justice White, had the support of Chief Justice Burger and Justices Stewart and Blackmun. Justice Brennan, who had dissented in *Lopez* concurred in the result, but only on the technical ground that *Katz* v. *United States* was not retroactive. Justice Black concurred in the judgement, but only because of his view that electronic surveillance is not a search and seizure subject to the Fourth Amendment. Dissenting opinions were filed by Justices Douglas, Harlan, and Marshall.

According to the plurality opinion, the question to be decided was this: what expectations of privacy are constitutionally "justifiable"—what expectations will the Fourth Amendment protect in the absence of a warrant? A police agent who conceals his identity may write down his conversations with a defendant and testify concerning them without a warrant. No different result, said the Court, is required if the agent records the conversations with electronic equipment carried on his person (as in *Lopez*) or carries radio equipment which tranmits the conversations to recording equipment located elsewhere or to agents monitoring the transmitting frequency (as in *On Lee* and in *White*).

The three dissenters, Justices Harlan, Douglas, and Marshall, objected to equipping agents with eavesdropping devices in the absence of a court order, but approved of use of informants without judicial supervision. Some critics suggested that "a far greater danger to our free society is presented by the prospect that friends and associates may be employed as government spies" than by equipping informants with electronic transmitting devices. The issue as Justice Harlan saw it in his dissenting opinion was whether "uncontrolled consensual surveillance in an electronic age is a tolerable technique of law enforcement, given the values and goals of our political system." He considered third-party monitoring a greater invasion of privacy than single-informant bugging. Third-party bugging, he believed, undermined that confidence and sense of security in dealing with one another that is characteristic of individual relations between individuals in a free society.

The dissent of Justice Douglas in *United States* v. *White* was much sharper than that of Justice Harlan. Justice Douglas could see no excuse for not seeking a warrant in the White case. He based his dissent not only on the Fourth Amendment ban on unreasonable search and seizure, but also on freedom of speech guaranteed by the First Amendment. Must everyone live in fear that every word he speaks may be transmitted or recorded, he asked. He could imagine nothing that has a more chilling effect on people expressing their views on important matters. (Consent eavesdropping and *White* are discussed more fully in "Eavesdropping on Trial", p.28 et seq.).

Several bills have been introduced in the House of Representatives to eliminate the exception of "consent eavesdropping" from court order requirements of Title III, and to permit a person to record electronically or otherwise intercept a wire or oral communication only where *all* parties to the communication have given prior consent to such interception (H.R. 9667; 9781; 9698; 9973; 10008; 10331). This is an ideal solution to a troublesome problem, but a proposal to outlaw warrantless consent eavesdropping will undoubtedly meet with fierce resistance by law enforcement officials and others. This type of electronic surveillance is reported to be used in tens of thousands of investigations each year. The practice is so firmly entrenched in law enforcement and the burden of dealing with crime is so great that public support for outlawing one-party-consent eavesdropping is far from certain. Businessmen and private individuals who routinely record telephone conversations can be expected to join in defending the practice.

DEFECTS IN COURT-ORDERED EAVESDROPPING

Seven problem areas of court-ordered eavesdropping have been identified that require attention by Congress or the courts and that must be solved if wiretapping and electronic surveillance by law enforcement officials is to be permitted to continue:

1. Offenses for which an order may be obtained are practically unlimited, and are not restricted to those characteristic of organized crime or serious offenses, despite the avowed purpose of the law.

2. The provision that the application and order shall describe the type of communication sought to be intercepted does not comply with Supreme Court requirements as to particularity.

3. Judge-shopping is possible, and there is opportunity for laxness in supervising interception of conversations.

4. Overhearing of innocent conversations and privileged communications under present procedures appears to be unavoidable and may be constitutionally impermissible.

5. The thirty-day period allowed for listening in, with an unlimited number of extensions each up to thirty days, may protract eavesdropping excessively and violate requirements of the Supreme Court.

6. The law is ambiguous as to who is to be notified of the eavesdropping, who may object, and when motions to suppress evidence may be made.

7. Reports required to be filled are inadequate to inform the public and to form the basis for evaluation of operation of Title III.

Both legal and practical problems are involved in these weaknesses of court-ordered eavesdropping under Title III, and each one of the seven problem areas will be discussed separately.

OFFENSES COVERED

The resaon for enactment of Title III of the Omnibus Act of 1968 offered most frequently and with greatest fervor by its supporters was, and still is, that it is an indispensable tool in fighting organized crime. Congress acknowledged this need in its introductory findings in the law. Critics of government eavesdropping insist that the law permits eavesdropping in investigation of many offenses that are not and will not be associated with organized crime. A long list of offenses for which *Federal* officers may seek a court order appears in Sec. 2516(1) of Title III:

(a) Offenses relating to espionage, sabotage, treason, riots, and enforcement of the Atomic Energy Act of 1954.

(b) Violation of Federal law restricting payments and loans to labor organizations, or offenses in labor racketeering.

(c) Bribery of public officials and witnesses and sporting contests, unlawful use of explosives, transmission of wagering information . . . obstruction of. . . law enforcement. Presidential assassinations, kidnapping and assault; interference with commerce by threats or violence; interstate and foreign travel or transportation in aid of racketeering; influencing operations of employee benefit plan . . . etc.

(d) Counterfeiting.

(e) Bankruptcy fraud; manufacture, importation, receiving, concealment, buying, selling, or dealing in narcotic drugs, marihuana, or other dangerous drugs.

(f) Extortion, including extortionate credit transactions.

(g) Conspiracy to commit any of the enumerated offenses.

These offenses were selected, according to the Senate Report on Title III, because they were characteristic of the activities of organized crime or because of their seriousness (No. 1097,p.97). However, eavesdropping in any offense seems to be sanctioned on the theory that organized crime has not limited itself to the commission of any particular offense.

The list of offenses in which *State* officials may obtain a court order is shorter, but perhaps even broader than that of the Federal government [Section 2516(2)]. The State list appears to be practically unlimited. State statutes may authorize eavesdropping in connection with: . . . . the offense of murder, kidnapping, gambling, robbery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year [or any conspiracy to commit any of these offenses.]

Except for the one-year imprisonment limitation in certain cases, the law appears to contain no limitation as to the nature of the offense covered. It may be argued that there is no need to limit the nature of the offenses. On the other hand, it must be recognized that there is great potential for abuse inherent in permitting eavesdropping over a wide spectrum of offenses. The open-ended clause "punishable by imprisonment for more than one year" has been attacked as an inaccurate way of distinguishing between serious and petty offenses.

Have court orders been obtained only for offenses characteristic of organized crime or serious offenses, the avowed targets of Title III? The nature of the offense for each court order granted and a summary of these offenses appear in each annual report to Congress by the Administrative Office of the United States Courts. At both Federal and State level, eavesdropping has been used most extensively in gambling and narcotics cases. Combined, these two offenses accounted for 85 percent of all court orders during 1971 and 1972. The reports do not reveal whether organized crime was involved or the seriousness of the offense. It is possible that many of the targets were small-time gamblers and narcotics peddlers, investigation of whom does not justify costly wiretapping or electronic surveillance.

Congress should take another look at the offenses for which a court order may be obtained. Invasion of privacy of innocent persons is inevitable in wiretapping and electronic surveillance. It may be justified in cases of organized crime and serious offenses where other investigative techniques are inadequate, but not in ordinary cases. Meanwhile, some self-restraint on the part of prosecuting officials and voluntary curbs on indiscriminate use of this powerful tool would seem to be in order.

SPECIFIC OFFENSE OR STRATEGIC INTELLIGENCE

An application for a court order must show that a *particular offense* has been, in being, or is about to be committed [Sec. 2518(1)(b)(1)]. This would seem to limit applications to those seeking specific information about a particular crime—that is, *tactical* as distinguished from *strategic* intelligence. Strategic intelligence consists of general information on the criminal activities of an individual that may enable officials to link him to other suspects or to some specific crime. Is strategic intelligence gathering outlawed by Title III? There is some justification for the view that it is banned. Perhaps Congress should reexamine this problem and attempt some clarification. The use of electronic devices to obtain strategic intelligence admittedly has great potential for abuse.

Eavesdropping for strategic intelligence is further complicated by Sec.2517(5) which permits interception and use of a communication relating to an offense other than that specified in the order if the judge finds, on *subsequent* application, that the contents of conversations were intercepted as provided by Title III. The United States Court of Appeals for the Tenth Circuit upheld this provision in *United States* v. *Cox* (449 F.2d 679 (1971)). In May 1972 the United States Supreme Court refused to hear an appeal, over the objection of Justice Douglas, Brennan, and Marshall (*Cox* v. *United States*, 405 U.S.932).

For a more detailed discussion of strategic and tactical intelligence, see "Eavesdropping on Trial," p.76 et seq. A bill introduced in the House of Representatives on December 7, 1973 (H.R.11838) appears to deal with this problem, but its purpose and wording require clarification.

THE PARTICULARITY REQUIREMENT

Title III requires that the application and order shall contain a particular description of the *type* of communication sought to be intercepted [Sec. 2518(1)(b) and Sec. 2518(4)(c)]. In *Berger* v. *New York* (388 U.S.41) however, one of the two 1967 landmark decisions of the Supreme Court with which Title III purports to comply, the Court made it clear that it was necessary "to describe with particularity the conversations sought," otherwise the officer would be given a roving commission to seize any and all conversations.

In litigation attacking the constitutionality of Title III, it is almost invariably claimed that merely describing the *type* of conversation does not comply with *Berger*. Since it is practically impossible to describe a particular conversation sought, especially in offenses of a continuing nature such as gambling and bookmaking, the prosecuting official is faced with a real dilemma. To comply fully with *Berger*, the particularly requirement of Title III would have to be narrowly construed, and strict enforcement would make the law practically unusable. Justice Black anticipated the problem of "particularity" in his dissenting opinion in *Katz* v. *United States* (389 U.S.347); he could not see how one could "describe" a future conversation. Justice Douglas has repeatedly observed that it would be extremely difficult to name a particular conversation to be seized and therefore any such attempt would amount to a general warrant,

the very abuse condemned by the Fourth Amendment (See *United States* v. *District Court*, 407 U.S. at p.333).

What does "type of communication" mean? If all that Title III requires is a statement of the nature of the offense to which the conversation is to relate, then the provision is meaningless, for details of the particular offense have already been set forth in the application and stated in the order. If it means a particular description of a particular conversation, then compliance may be impossible. The meaning of "type of communication" takes on added importance by the requirement in Title III that interception must end automatically when the described type of communication has first been obtained, unless the application shows probable cause to believe that additional communications of the same type will occur later [Sec.2518(1)(d)].

The issue of "particularity" may eventually be settled by the United States Supreme Court. Meanwhile, Congress might effect some clarification by requiring that an applicant for a court order describe the communications sought to be intercepted as specifically and in as detailed a manner as possible. This would discourage the practice of merely repeating the nature of the offense that is being investigated.

JUDGE-SHOPPING FOR COURT ORDERS

A heavy burden is placed on Federal and State judges to whom applications for court orders are presented. Before he signs an order to wiretap or conduct electronic surveillance, the judge must determine whether all the requirements of the law are satisfied. He must make findings as to "probable cause" and decide if the facts in the application show that normal investigative procedures have been tried and failed, or reasonably appear to be unlikely to succeed if tried or to be too dangerous [Sec.2518(3)(c)]. An order may require periodic reports to the judge showing what progress has been made and the necessity for continued interception. Judges have responsibility for safeguarding the records. The law also gives the judge discretionary power to decide whether certain individuals shall be notified of the eavesdropping, and what portions of the recordings shall be made available for inspection.

The onerous duties and responsibilities of the judge in government eavesdropping make it an unattractive job to sign an order, even for those Federal or State judges who favor this technique of law enforcement. The prosecuting official who wants a warrant to wiretap or use electronic surveillance must find a judge who is willing to issue it and take on all the judicial duties imposed by the law. A wide choice is open to the applicant, for an order may be signed by any judge of competent jurisdiction. This is defined in Sec. 2510(9) as: (a) A judge of the United States district court or a United States court of appeals; and (b) A judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire or oral communications.

No safeguard against "judge-shopping" is provided by Title III. Practical necessity forces applicants to pick a judge who is known to be receptive to eavesdropping and at least reasonably lenient in signing orders. Selection of a friendly judge is almost always possible, particularly in State practice. If law enforcement officials can shop around for a complaint and undemanding judge, the dangers of abuse of privacy through eavesdropping may be greatly increased. How is this to be remedied? Competent, alert, and aggressive judges are the key to maintaining the safeguards provided by law.

Congress cannot control the caliber of State judges, or even the Federal judiciary. It can, however, remedy one obvious gap in judicial supervision of court-ordered eavesdropping: *progress reports* to judges should be *mandatory* and not discretionary. The Act now provides that an order *may* require periodic reports to the judge showing what progress has been made and the necessity for continued interception [Sec.2518(6)]. Progress reports are intended to serve as a check on the continuing need to conduct the surveillance and to prevent abuse. Federal judges are reported generally to require progress reports. Few, if any State judges have specified in the court order that progress reports shall be submitted, although some say that they receive oral progress reports from time to time. This may seriously undermine judicial supervision of the operator who is listening to intercepted conversations and of the law enforcement official who is handling the investigation.

OVERHEARING INNOCENT OR PRIVILEGED CONVERSATIONS

Congress knew that government eavesdropping would inevitably result in intercepting innocent conversations and tried to deal with the problem. The law requires that "every order and extension . . . shall contain a provision that [it] shall be conducted in such a way as to minimize the interception" of innocent conversations [Sec.2518(5)]. How is it to be kept to a minimum? The law does not say, other than to limit the time period of interception and to require that it terminate "upon attainment of the authorized objective.

Those who opposed passage of Title III in 1968 were particularly concerned that many irrelevant and innocent conversations would be overheard. Unfortunately, their apprehensions appear to have materialized in both Federal and State practice. Monitoring agents have not been trained adequately to recognize innocent conversations as such and to stop recording them. They simply do not know when to stop listening. Administrative regulations are needed to control the agents who man the monitoring devices. For recommendations of the American Bar Association, see "Eavesdropping on Trial", pp.215–216.

The problem of overhearing many innocent conversations is further complicated by the fact that Title III does not state clearly that automatic recording is barred and that live monitoring must be used. In *automatic recording* conversations are recorded on tapes without listeners and are later played back at intervals, the frequency depending on the circumstances and on the practice established in a particular office. The automatic device records *all* conversations. In *live monitoring*, also called "manual recording", police officers or agents sit continuously at the receiving station, listening to the recordings and making notes of relevant conversations on a typewriter or in longhand. The recorder can be shut off when innocent, irrelevant, or privileged conversations are taking place, if they can be recognized as such.

Before 1968, in States where court-ordered eavesdropping was permitted, it was common practice to use automatic monitoring and play back the record at twenty-four-hour intervals. Since Title III requires that a wiretap cease when the conversation sought has been obtained, and that the interception be conducted in such a way as to minimize interception of communications not covered by the court order, it would appear that automatic monitoring is now illegal. Monitoring is done by agents or police officers whose knowledge, judgment, and integrity cover a wide range. Each person interviewed was asked whether he used live monitoring or automatic recording. Those convinced that live monitoring is required by the 1968 law said they always use it. Those who were unaware or uncertain of the need for live monitoring furnished answers indicating that automatic recording is still used (see "Eavesdropping on Trial" pp. 126–128, 164]. This is a matter that could be clarified by Congress. Automatic recording should be banned.

A disproportionate number of innocent conversations seems to have been overheard in some cases; in one investigation reported to the Administrative Office of the United States Courts, 400 telephone calls were intercepted to get one incriminating conversation; in another over 1,000 for 20. In a third case 1,342 intercepts were reported to have been made, not a single one of which was incriminating. Even if police officers are instructed not to listen to non-incriminating conversations, no guidelines are available to determine whether a conversation is "criminal" or not. Some administrative regulations are needed to control extended interception of innocent conversations by monitoring agents. Training programs have been suggested by the Law Enforcement Assistance Administration, but the LEAA's authority to put such programs into effect is limited.

Overhearing *privileged communications*, such as conversations between doctor and patient, attorney and client, priest and penitent, is a problem that parallels interception of innocent conversations, although it does not happen as frequently. Sec.2517(b) of Title III provides that such communications shall not lose their privileged character whether the interception is lawful or unlawful. This attempt to protect privileged communications does not appear to have been very successful. Most monitoring agents are ill-equipped to decide when a communication is privileged and to stop listening, and the United States Department of Justice is reported to have issued instructions to record all conversations, including privileged communications (see "Eavesdropping on Trial," p. 160).

TIME PERIOD FOR INTERCEPTION OF CONVERSATIONS

A court order may allow interception of conversations to continue for a period up to thirty days, with an unlimited number of thirty-day extensions [Sec. 2518(5)]. The time length raises policy as well as constitutional problems. Should it be so long? In *Berger* v. *New York*, the Supreme Court disapproved of surveillance over a period of sixty days and called it "indiscriminate seizure." In *Katz* v. *United States*, the Court turned to a case-by-case approach; in this instance interceptions covered a very brief period. A narrow construction of *Berger* would seem to indicate that interception for an entire thirty-day period, particularly with extensions, constitutes a general search and is therefore unconstitutional.

Many State court orders have provided for interception during the maximum thirty-day period, and renewals have been granted freely. Federal orders, on the other hand, have generally limited the period to fifteen days. United States law enforcement officials expressed the opinion that if applications were more conservative than the law required and asked for a shorter period of interception than permitted by Title III, the prospects for sustaining the wiretap in the courts would be improved.

Requests for orders covering a longer period than is necessary frustrate the specific requirements of the law. State and Federal officials claim that an extended period is needed where the offense is a continuing one, but some admitted frankly that extensions were sometimes asked in order to postpone giving notice of the interceptions. It may be argued that the thirty-day period does not square with *Katz in United States in* which the Supreme Court expressed approval of interception of specific, not continuous conversations. The granting of an unlimited number of thirty-day extensions also gives rise to the suspicion that a law enforcement official may be engaging in "strategic intelligence" surveillance instead of attempting to obtain specific evidence of a crime.

Congress should reconsider the time period allowed for interceptions in Title III. The conservative section of the American Bar Association (ABA) recommended a maximum initial period of fifteen days in 1971; the more liberal Criminal Law Council of the ABA proposed a reduction to five days, with one extension of five days. The American Civil Liberties Union would like to see all renewals of court orders eliminated. A compromise in reduction in the time period allowed for interception conversations should not be too difficult for Congress to reach.

H.R.13825 introduced in the House of Representatives by Mr. Kastenmeier with respect to "national security" eavesdropping limits the period of a court order to "no longer than is necessary to achieve the objective of the authorization nor in any event longer than fifteen days." An extension of the order is limited to ten days in H.R. 13825. This would seem to be a reasonable period of time for *all* court-ordered eavesdropping.

NOTICE OF EAVESDROPPING, OBJECTIONS, AND DISCLOSURES

Serious ambiguities are created by the provisions of Title III requiring notice of eavesdropping and permitting aggrieved persons to object to the use of evidence obtained. Some injured persons may never be given notice, and it is not clear who has "standing" to object or what should be disclosed. The law requires that notice shall be given no later than ninety days after termination of interception to the persons named in the order or application. In the discretion of the judge, other parties to intercepted conversations may also be given such notice "in the interest of justice" [Sec.2518 (8)(d)].

The purpose of the notice is to give "aggrieved persons" an opportunity to make objections by a motion to suppress evidence. An aggrieved person is defined as anyone "who was a party to any intercepted wire or oral communication or . . . against whom the interception was directed" [Sec.2510(11)]. Under this definition, an individual may be incriminated by an unlawful interception and yet have no "standing" to object. A person may be "aggrieved," yet the judge may decide that no notice shall be given to him. Furthermore, the notice need not state exactly *what* conversations were intercepted; it is left to the judge to determine what portions, if any, of the overheard conversations shall be available for inspection. The duty of causing service of the notice is placed on the judge, and he may postpone it indefinitely.

Title III is also ambiguous as to *when* an aggrieved person may move to suppress evidence obtained by eavesdropping. Section 2518(10)(a) says it must be made "before the trial, hearing or proceeding," unless there was no opportunity to do it or the person was not aware of the grounds of the motion. Is the motion premature if made before arrest and indictment?

Some of the uncertainties with respect to notice, objections, and disclosure may be clarified by the courts, but this is one aspect of Title III of the Omnibus Act of 1968 that could profit from legislation by Congress. The law leaves much to the discretion of the judge, but the judge really relies on the law enforcement official handling the case. Some officials circumvent the effects of the notice requirement, or at least postpone it, by asking for extensions of the court order. New probable cause as to why the wiretap should be continued must be shown, but this does not seem to be too difficult to do, judging from the number of extensions granted. Judges must rely on the law enforcement officials and appear to be easily convinced that an extension is necessary.

The following proposals deserve serious consideration by Congress: (1) make mandatory the giving of notice to individuals whose wire or oral communications have been intercepted, within thirty days after expiration of the court order; (2) limit the power of the judge to postpone giving notice, particularly where the individual whose communication is intercepted is not engaged in a continuing criminal enterprise; (3) require that persons entitled to notice be given, on request, a copy of the order and application, and information as to conversations overheard. These proposals are included in H.R.13825 introduced in the House of Representatives by Mr. Kastenmeier on March, 1974 and cited as "Surveillance Practices and Procedures Act of 1974."

REPORTS ON COURT-ORDERED EAVESDROPPING

Three reports are required by Sec.2519 of Title III:

1. Report by the judge issuing or denying an order, within thirty days after expiration of the order or its denial.

2. Report by prosecuting officials in January of each year on each application for an order or extension during the preceding year.

3. Annual report to Congress by the Administrative Office of the United States Courts in Washington, D.C., in April of each year, on the number of applications and orders and a summary and analysis of the data required to be filed with it by judges and prosecuting officials.

The reports of judges and prosecuting officials, both Federal and State, are made to the Administrative Office of the United States Courts. This Office, in turn, collates the information obtained and renders a report to Congress that is largely statistical. The system set up in Title III for filing reports was designed to keep Congress and the public informed as to the extent of eavesdropping throughout the United States, offenses for which it was used, manner in which surveillance was conducted, identity of prosecuting officials who applied for orders and judges who signed them, cost, and the results of interceptions. It was also to serve as a basis for evaluation of effectiveness of operation of Title III by a 15-member Commission scheduled to come into existence after the law had been in effect for several years. This Commission is now in the process of formation.

All three reports have been widely criticized on the ground that they neither inform adequately nor furnish sufficient data for meaningful evaluation of eavesdropping under Title III. Much of the criticism appears to be justified. Prosecuting officials and judges use a standard form of report prepared by the Administrative Office of the United States Courts to comply with Title III requirements pursuant to regulations issued by that Office. Some of the items in the form of report are vague and convey no significant information. Many law enforcement officials do not take the reports very seriously, and judges are inclined to find them a nuisance and leave the job of filling in the form to the prosecuting official. At least six items in the report of prosecuting officials have been identified as lacking in clarity:

1. *Average frequency of intercept per day.*—Suppose during a thirty-day period no interceptions occurred, except on the last day when there were thirty interceptions. Is the average frequency one? How could such an average be of any significance? This item might be improved to require a statement of the

total number of days in which interceptions actually occurred, out of the total number of days authorized.

2. *Number of persons whose communications were intercepted.*—Does this mean the number of people using that particular phone or calling that number, whether or not their conversations were relevant to the matter under investigation?

3. *Number of communications intercepted.*—Suppose calls are made, but nobody picks up the telephone, as often happens. Is the telephone number called to be counted as an interception? I believe that attempted as well as concluded calls should be included.

4. *Number of incriminating communications intercepted.*—What is an incriminating conversation? A phones B and says: "I will meet you in ten minutes." Is this incriminating? If one wants to show that many incriminating statements are overheard in order to prove that court-ordered wiretapping and electronic surveillance are effective, many calls can be included as "incriminating" that others may find innocent.

5. *Number of convictions.*—A conviction may be obtained in a case subject to a wiretap order, but this does not mean that the conviction resulted from the wiretap. Officials should be required to indicate whether conversations intercepted were used as evidence in obtaining a conviction, and whether in their opinion these intercepted communications contributed substantially to conviction. They should also indicate what other investigative techniques were used.

6. *Cost.*—Some prosecuting officials find this item so ambiguous and troublesome that they leave it blank. It should be made clear that a statement is required of the exact amount paid to each investigator and all other individuals who spent time on the particular wiretap. It should include cost of equipment, plant, and any other items of expense involved in intercepting conversations, recording, and making logs and transcripts. Only by strict adherence to this requirement can evaluation of eavesdropping on the basis of cost be meaningful.

The Annual Report to Congress has been useful in publicizing the number of court orders issued, the geographic areas in which eavesdropping (predominantly wiretapping) has taken place, the names of prosecuting officials who applied for court orders and the judges who signed them, and the general nature of offenses involved. Criticism has focused on the summary and analysis by the Administrative Office of: (1) the number of incriminating conversations intercepted, and (2) cost.

The Report to Congress submitted at the end of April 1973 states that "approximately one-half of the conversational intercepts produced incriminating evidence." The report stresses averages; only a close look at each listing would reveal that in one Federal case only 10 out of 500 intercepts were incriminating (2%), and in another case 3 out of 191 intercepts (.015%); in a third, none out of 1,342 (0%). Congress and the public should be made aware of the limitations of the Annual Report and its potential for providing misleading information.

As to cost, the Annual Report to Congress summarizing reports of prosecuting officials and judges for the year 1972 indicated that the cost of an intercept ranged from $5 to $82,628, and that the average cost for 805 orders *for which cost was reported* was $5,435. What evaluate purpose can be served by such statistics, without relating cost to the results of the intercepts?

No information is included in any report with respect to forty-eight-hour emergency wiretaps without court order or warrantless eavesdropping in so-called "national security" cases.

EVALUATION OF EAVESDROPPING UNDER TITLE III

Wiretapping and electronic surveillance by Government can be justified, according to its supporters, by a *balancing* process. The individual's right of privacy and freedom in a democratic society has to be baanced against the needs of law enforcement and the effectiveness of eavesdropping. Equilibrium is achieved, it is claimed, when official eavesdropping is permitted, with adequate safeguards to protect privacy.

The balance approach to the problem of governmental intrusions into privacy is difficult to apply. To strike a balance between competing interests, the elements on both sides must be measurable and capable of being weighed in similar terms. The right to privacy and freedom, however, does not lend itself to accurate measurement. Nor is it easy to assess either need or effectiveness of eaves-

dropping in establishing "law and order." What questions must be asked to determine if an acceptabe balance has been reached?

As to the *right to privacy*, one must ask whether intrusions against innocent persons have been minimized by the safeguards provided by the law and have been carried out in practice. Some weight must also be given to the potential for abuse inherent in wiretapping and electronic surveillance and to whether Title III has reduced illegal eavesdropping. As to law enforcement *needs* and *effectiveness* of eavesdropping, it must be determined whether public security has been strengthened by use of Title III against organized crime and serious offenses. Has the law been used against the targets intended, and has it resulted in convictions of top echelon offenders. The sensitivity of the pubilc in a society that places a high value on "freedom" must also be considered in weighing the right of privacy against law enforcement needs, and this depends on who are the subjects of surveillance and for what purpose wires have been tapped.

MINIMIZING INVASION OF PRIVACY

Invasion of privacy can be reduced to some extent by limiting the duration of court orders to a short period, restricting them to serious cases where less intrusive tools of law enforcement are clearly not serviceable, and supervising monitoring of conversations closely. Court orders under the 1968 law, most of them for wiretapping, have authorized interceptions for periods that appear excessive; they have been extensively against individuals in all levels of gambling and narcotics, and supervision of monitoring agents has not been very stringent.

The most careful scrutiny by an impartial judge of applications for court orders, and continued judicial concern throughout the period of the order, are essential if safeguards are to be meaningful and invasion of privacy is to be kept to a minimum. The ease with which it is possible to go to a friendly judge who will sign an order for whatever period a prosecuting officer asks, and the failure of State judges to require written progress reports, leave the door open to unjustified invasions of privacy. The conclusion is inescapable that to the extent that safeguards provided by Title III are ambiguous, the statute as enacted is inadequate in protecting the right to privacy. Insofar as the ideal of continuing scrutiny by an impartial magistrate has not been realized in practice, the protections against undue invasion of privacy have not been fully applied. In balance, privacy has been weakened.

Has Title II reduced *illegal eavesdropping?* The truth is that there really is no way of knowing how much illegal eavesdropping has been going on. Each person interviewed in obtaining data for my study and report on eavesdropping under Title III was asked whether he beieved that investigating agents were eavesdropping illegally despite Title III which makes legal wiretapping and electronic surveillance available. Some said illegal eavesdropping was possible, others said it was probable, and a few were positive that conversations not covered by court orders were being intercepted (see "Eavesdropping on Trial," p.199). Those who favor eavesdropping under Title III are inclined to minimize the potential for abuse; those who oppose it are sure that illegal eavesdropping is extensive. There is no hard evidence to indicate that Title III has made any appreciable difference either in increasing or reducing illegal eavesdropping, but the temptations for illegal eavesdropping under color of law cannot be ignored.

THE NEED FOR EAVESDROPPING

Opinion has been and continues to be divided on the need for wiretapping and electronic surveillance in law enforcement. Before Title III was enacted in 1968, many law enforcement officials testified in Congressional hearings that eavesdropping was an indispensable tool in dealing with organized crime. Others claimed it was a costly, wasteful, lazy-man's weapon, a threat to innocent persons, and useless against top echelon criminals. No one has ever succeeded in proving need, or even in defining it cearly. Nor has it ever been settled who should hear the burden of proving need. How, then, is need to be weighed in a balancing process? As a start, alternatives to eavesdropping would have to be analyzed, and time and cost factors compared. Would the same resources devoted to normal types of surveillance produce equal or better results or no results at all? If Title III has not been used effectively against organized crime or limited to serious offenses, the need for eavesdropping to promote public safety is weakened in balancing it against invasion of privacy.

Operation of Title III since 1968 has demonstrated neither need nor lack of need for eavesdropping. Nor does the information required to be furnished in reports under Title III further the examination and analysis of need.

EFFECTIVENESS OF EAVESDROPPING UNDER TITLE III

Has Title III been effective? If it has not, then the balance is tipped in favor of the right of privacy and against wiretapping and electronic surveillance in law enforcement. "Effectiveness" is a vague concept. One factor that Congress seems to have considered significant in "effectiveness" is the number of arrests and convictions that result from eavesdropping. This item of information must be included in the report of the prosecuting official [Sec.2519(2)(c)(f)]. But the reports do not show any meaningful relation between eavesdropping and arrests or convictions. If a court order to wiretap has been obtained in a case and eventually a conviction results, does this mean that the wiretap was "effective"? The wiretap may have produced no useful evidence and the conviction may have been obtained on evidence secured by other investigative techniques. The law requires the prosecuting official's report to include "a general assessment of the importance of the interceptions," but the forms examined personally by me revealed that this item is frequently left blank.

Those who favored eavesdropping before the law was passed now claim it is effective. Those who opposed it question the adequacy of the statistics that purport to show effectiveness. Law enforcement officials are inclined to say that arrests and convictions could not have been obtained without wiretapping. Critics of government eavesdropping, however, can always cite important investigations in which it proved to be of insignificant or no value compared with normal techniques.

It can be conceded that eavesdropping has been effective in some cases in obtaining arrests and convictions. This does not prove that other methods of surveillance would not have been equally productive. Nor, in determining effectiveness of Title III, can the quaity of an arrest or conviction be ignored. If Tite III has been successful in apprehending only small-time offenders and has failed to reach leaders of organized crime, then court-ordered eavesdropping has missed its mark.

Title III has been used most extensively in gambling and narcotics cases. Criminologists claim that the efforts of law enforcement in offenses such as these, which involve willing participants, can have only limited effectiveness, no matter what tools are used. So long as the public wants the services provided and the demand is not satisfied through awful channels, the illegal activities will continue. Sociologists are inclined to agree; they deplore the tendency of forces favoring government wiretapping and electronic surveillance to deny the relationship between crime, slums, and poverty.

Since *need* and *effectiveness* are such elusive elements and defy accurate measurement, some other factors must be found if the balancing process is used in evaluating eavesdropping. Perhaps one should weigh competing *values*. Is the apprehension of some crimina suspects worth the risks to privacy inherent in eavesdropping? If wiretapping and electronic surveillance are allowed under a law that is ambiguous, and carried on without clear standards and uniform guidelines by a large number of officials in a wide variety of cases without adequate controls, the risks may be too great.

The 15-member "National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance" provided for by Sec.804 of the Omnibus Crime Control and Safe Streets Act of 1968 (as amended in 1970), has come into existence. The President of the United States has appointed seven members; four members of the Senate have been appointed by the President of the Senate. The Speaker of the House of Representatives has not yet designated the four remaining members of the Commission from the House. The Commission is to file a report within two years after its formation and then go out of existence.

The function of this Commission is "to conduct a comprehensive study and review of the operation of the provisions" of the law in order to determine its "effectiveness." Does "operation" refer only to procedures and practice, without consideration of ambiguities in the aw? The scope of the Commission's function does not seem to include the extent of governmental intrusion and whether eavesdropping has been excessive. The "need" for wiretapping and electronic surveillance seems to be assumed; the Commission is instructed only to deal with "effectiveness."

Is the Commission to consider whether Title III has been effective in banning *private eavesdropping?* Effectiveness of the law prohibiting interceptions by private individuals must depend largely on receipt of complaints and vigorous enforcement. State officials report that few, if any, complaints have been received since passage of Title III. Detection of unlawful wiretapping is difficult, and it may be even harder when an electronic device is installed. The Department of Justice appears to have been more active than the States in dealing with private eavesdropping under Title III, but few prosecutions have resulted. For a discussion of the ease with which the ban on private eavesdropping can be circumvented, see "Eavesdropping on Trial", pp.42–43.

Congress should give serious consideration to creation of an impartial, unbiased, non-political agency on a continuing basis to oversee government eavesdropping. The Commission provided for by Title III has a limited life for a narrow and rather ambiguous purpose, and its composition makes it vulnerable to political pressure. Government eavesdropping has great potential for abuse. as we all know by now. If wiretapping and electronic surveillance by law enforcement officials is to be allowed to continue under law, periodic check of Federal and State practices is essential.

No meaningful evaluation of eavesdropping under Title III can be made by *any* Commission without taking into account ambiguities in the law, lack of clear standards, and failure to establish uniform guidelines; these may create threats to privacy and liberty that are intolerable in a free society. A review of Title III must ferret out information in the field, beyond the statistical data in the reports. In addition to examining whether the protections offered by the law are adequate, it must be determined whether they have been weakened in practice. Modifications are surely needed in both law and procedure.

SUMMARY OF PROPOSALS

Congress has sanctioned government eavesdropping as a law enforcement tool, and Americans must live with—at least until Congress repeals Title III of the Omnibus Crime Control and Safe Streets Act of 1968, the Supreme Court declares it unconstitutional, or the Executive orders its agencies not to use it. Since none of these events is likely in the foreseeable future, the attention of Congress and the public must be directed to minimizing invasion of privacy and maximizing meaningful law enforcement by correcting defects in the law and weaknesses in practice. The following proposals are made with full awareness of the conflict between the two objectives—protecting privacy and dealing with crime—and the difficulties in reconciling them.

1. Clarify ambiguous provisions of Title III, particularly with respect to: persons entitled to notice that eavesdropping has taken place; when motions to suppress evidence may be made; what conversations are to be deemed "incriminating;" what is meant by "type" of communication to be set forth in the application and order; gathering of "strategic intelligence," use of live monitoring and banning of automatic recording.

2. Limit eavesdropping to organized crime and serious offenses. Perhaps Congress should consider amending Title III to define "organized crime" and "serious" offenses.

3. Establish uniform procedures and standards for Federal and State officials. Automatic recording should be eliminated immediately as a matter of practice, without waiting for legislation to that effect. Progress reports to judges should be made mandatory by law; meanwhile judges should be urged to require them. The time period requested for court orders should be as short as possible, and legislation should be introduced to limit the period to fifteen days, with one renewal of ten days—except possibly on a clear showing that the offense is a continuing one and that additional extension is required. Congress should consider authorizing administrative regulations to control agents who man the monitoring devices. The Law Enforcement Assistance Administration should be urged to prepare and carry out training programs.

4. Improve reporting requirements. Congress should consider amendment of Sec.2519 of Title III to clarify the information to be furnished by prosecuting officials as indicated in this Statement. The Annual Report to Congress should also be clarified.

5. Check Federal and State practices periodically. This should be done by a watchdog with no vested interest in the success or failure of Title III. A permanent agency should be empowered to make periodic examinations of

Federal and State statutes and procedures, and hold public hearings on law and practice. The inquiries of this agency must be independent and go beyond the statistical reports and summaries submitted to Congress annually.

These are minimal proposals to restore a balance between the rigift of privacy and law enforcement requirements. Not much more than a year ago, a knowledgeable and experienced member of the House of Representatives estimated that not more than forty Congressmen could be induced at that time to consider any amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968. The prospects for remedying defects and weaknesses in the law in both House and Senate appear to have improved considerably. The public has become painfully aware that widespread wiretapping and electronic surveillance, legal and illegal, are a serious threat to personal liberty. The great potential for abuse and misuse in official eavesdropping has cast its shadow on the purported safeguards provided in Title III. If the law is not clear, if the power of surveillance is diverted to unintended purposes, if it is used indiscriminately for minor offenses, eavesdropping as a tool of law enforcement can be completely lost.

H.R. 9781 introduced late in 1973 in the House of Representatives is, in effect, a reaffirmation of the right of privacy and complete rejection of government wiretapping and electronic surveillance. Banning government eavesdropping may not have present appeal in the face of rising crime, but the pendulum may swing the other way if defects in law and practice are not cured. Clarity in the law, promulgation of uniform standards and guidelines, strictest conformity by officials with all available safeguards, and constant vigilance by Congress, the Courts, and the public are imperative if the right of privacy and the lawful use of eavesdropping as a tool of law enforcement are both to survive.

UNITED STATES SUPREME COURT DECISIONS

[Subsequently, the following report was received from the Department of Transportation:]

DEPARTMENT OF TRANSPORTATION,
OFFICE OF THE SECRETARY OF TRANSPORTATION,
Washington, D.C., May 13, 1974.

Hon. PETER W. RODINO, JR.
Chairman,
Committee on the Judiciary,
U.S. House of Representatives,
Washington, D.C.

DEAR MR. CHAIRMAN: The Department of Transportation would like to take this opportunity to offer to the Committee our views on H.R. 9815 and H.R. 11629, bills

"To enforce the first amendment and fourth amendment to the Constitution, and the constitutional right of privacy by prohibiting any civil or military officer of the United States or the militia of any State from using the Armed Forces of the United States or the militia of any State to exercise surveillance of civilians or to execute the civil laws, and for other purposes."

These bills would add a new section, 1386, to chapter 67 of title 18, United States Code, to prohibit the use of the armed forces of the United States, with certain exceptions, for investigation or surveillance of any person not a member of the armed forces, or of any civilian organization, regarding their beliefs, associations, or political activities. An amendment to chapter 171 of title 28, United States Code, would authorize individuals to bring a civil action for damages and obtain other equitable relief for violation of the proposed section

1386 of title 18 and to permit class actions to enjoin those activities. These bills would also amend the Posse Comitatus Act (18 U.S.C. 1385) to bring the Coast Guard, Navy, and Marine Corps within the coverage of that statute.

Within this Department, the Coast Guard conducts investigations relative to our statutory responsibilities which would be adversely affected by these bills. These investigations are conducted in the following areas:

a. Investigations to assist the Coast Guard in the performance of its powers, duties, or functions under the general authority of the Commandant (14 U.S.C. 93(e));

b. Criminal investigations under the implied authority of the Uniform Code of Military Justice (10 U.S.C. 831);

c. Investigations relating to the general law enforcement and security responsibilities of the Coast Guard (14 U.S.C. 2, 89, and 91, and 50 U.S.C. 191);

d. Investigations regarding civilian personnel security conducted under Executive Order 10450;

e. Surveillance of vessels under sections 101(4) and 101(8) of the Ports and Waterways Safety Act (33 U.S.C. 1221 *et seq.*);

f. Special surveillance over certain foreign vessels which enter United States ports, in accordance with Executive Order 10173 and National Security Decision Memorandum 82 (as authorized by 50 U.S.C. 191);

g. Investigations pursuant to the administrative of the laws relating to merchant vessel personnel (46 U.S.C. 214, 221-249, and 50 U.S.C. 191); and,

h. Investigations pursuant to the review of marine casualties (33 U.S.C. 1223 and 46 U.S.C. 239).

Due to the Coast Guard's role as an organization with both civil and military responsibilities, the impact of these bills on the Coast Guard differs substantially from their impact on the other armed forces. If the Coast Guard is to effectively meet its responsibilities, it is essential that the authority for these investigatory and surveillance functions not be unduly restricted. We, therefore, object to these bills insofar as the prohibitions proposed therein would be applied to the Coast Guard. If these bills were to be considered favorably, we would recommend that section 2 be amended to exclude the Coast Guard by using a phrase other than "armed forces" which is defined in these bills and 10 U.S.C. 101(4) as including the Coast Guard.

Section 5 of these bills would expand the scope of the Posse Comitatus Act to include the Coast Guard. We do not object to this change. It would not inhibit the Coast Guard from carrying out its historic law enforcement duties as they are specifically authorized by Acts of Congress, including 14 U.S.C. 89; and therefore fall within the exception to 18 U.S.C. 1385.

The Office of Management and Budget advises that, from the standpoint of the Administration's program, there is no objection to the submission of this report to the Committee.

Sincerely,

RODNEY E. EYSTER,
General Counsel.

Mr. KASTENMEIER. Until the committee at some point in the future reconvenes for consideration of this question, the subcommittee stands adjourned.

[Whereupon, at 1:10 p.m. the subcommittee was adjourned, subject to the call of the Chair.]

○