Calendar No. 1094

94TH CONGRESS
2d Session

SENATE

REPORT
No. 94-1161

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1976

AUGUST 24 (legislative day, AUGUST 23), 1976.—Ordered to be printed

MR. INOUYE, from the Select Committee on Intelligence, submitted the following

REPORT

together with

ADDITIONAL VIEWS

[To accompany S. 3197]

The Select Committee on Intelligence, to which was referred the bill (S. 3197) to amend title 18, United States Code, to authorize applications for a court order approving the use of electronic surveillance to obtain foreign intelligence information, having considered the same, reports favorably thereon with amendments and recommends that the bill, as amended, do pass.

AMENDMENTS

On page 2, strike out all after line 8 through the end of Section "2121" at page 4, line 20, and insert in lieu thereof the following:

(1) "Foreign power" means—

(A) a foreign government or any component thereof, whether or not recognized by the United States;

(B) a faction of a foreign nation or nations, not substantially composed of permanent resident aliens or citizens of the United States;

(C) an entity, which is directed and controlled by a foreign government or governments;

(D) a foreign-based terrorist group; or

(E) a foreign-based political organization not substantially composed of permanent resident aliens or citizens of the United States.

(2) "Agent of a foreign power" means—

57-010

(A) a person who is not a permanent resident alien or citizen of the United States and who is an officer or employee of a foreign power;

(B) a person who—

(i) knowingly engages in, or knowingly acts in furtherance of, terrorist activities for or an behalf of a foreign power, or

(ii) conspires with, aids, or abets such a person, knowing that such person is engaged in such activities;

(C) a person who—

(i) knowingly engages in, or knowingly acts in furtherance of, sabotage activities for or on behalf of a foreign power, or

(ii) conspires with, aids, or abets such a person, knowing that such person is engaged in such activities;

(D) a person who—

(i) knowingly engages in clandestine intelligence activities for or on behalf of a foreign power, which activities involve or will involve a violation of the criminal statutes of the United States; or

(ii) conspires with, aids, or abets such a person, knowing that such person is engaged in such clandestine intelligence activities; or

(E) a person who, acting pursuant to the direction of an intelligence service or intelligence network which engages in intelligence activities in the United States on behalf of a foreign power knowingly transmits information or material to such service or network in a manner intended to conceal the nature of such information or material or the fact of such transmission under circumstances which would lead a reasonable man to believe that the information or material will be used to harm the security of the United States, or that lack of knowledge by the Government of the United States or such transmission will harm the security of the United States.

(3) "Terrorist activities" means activities which—

(A) are violent acts or acts dangerous to human life which are criminal under the laws of the United States or of any State if committed within its jurisdiction; and

(B) appear to be intended—

(i) to intimidate or coerce the civilian population, or

(ii) to influence the policy of a government by intimidation or coercion.

(4) "Sabotage activities" means activities prohibited by title 18, United States Code, section ____, chapter 105.

(5) "Foreign intelligence information" means—

(A) information which relates to, and is deemed necessary to the ability of the United States to protect itself

against, actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) information with respect to a foreign power or foreign territory, which relates to, and because of its importance is deemed essential to—

(i) the national defense or the security of the Nation, or

(ii) the conduct of the foreign affairs of the United States;

(C) information which relates to, and is deemed necessary to the ability of the United States to protect against the terrorist activities of a foreign power or an agent of a foreign power;

(D) information which relates to, and is deemed necessary to the ability of the United States to protect against the sabotage activities of a foreign power or an agent of a foreign power; or

(E) information which relates to, and is deemed necessary to the ability of the United States to protect itself against, the clandestine intelligence activities of an intelligence service or network of a foreign power or an agent of a foreign power.

(6) "Electronic surveillance" means—

(ii) conspires with, aids, or abets such a person, knowing that such person is engaged in such activities involve or will involve a violation of the criminal statutes of the United States; or

(D) a person who—

(i) knowingly engages in clandestine intelligence activities for or on behalf of a foreign power, which activities involve or will involve a violation of the criminal statutes of the United States; or

(ii) conspires with, aids, or abets such a person, knowing that such person is engaged in such clandestine intelligence activities; or

(E) a person who, acting pursuant to the direction of an intelligence service or intelligence network which engages in intelligence activities in the United States on behalf of a foreign power knowingly transmits information or material to such service or network in a manner intended to conceal the nature of such information or material or the fact of such transmission under circumstances which would lead a reasonable man to believe that the information or material will be used to harm the security of the United States, or that lack of knowledge by the Government of the United States or such transmission will harm the security of the United States.

(3) "Terrorist activities" means activities which—

(A) are violent acts or acts dangerous to human life which are criminal under the laws of the United States or of any State if committed within its jurisdiction; and

(B) appear to be intended—

(i) to initimate or coerce the civilian population, or

(ii) to influence the policy of a government by intimidation or coercion.

(A) the acquisition, by an electronic, mechanical, or other surveillance device, of the contents of a wire communication to or from a person in the United States, without the consent of any party thereto, where such acquisition occurs in the United States while the communication is being transmitted by wire;

(B) the acquisition, by an electronic, mechanical, or other surveillance device of the contents of a radio communication, without the consent of any party thereto, made, under circumstances where a person has a constitutionally protected right of privacy and where both the sender and all intended recipients are located within the United States; or

(C) the installation or use of an electronic, mechanical, or other surveillance device in the United States to acquire information other than from a wire communication or radio communication under circumstances in which a person has a constitutionally protected right of privacy.

(7) "Attorney General" means the Attorney General of the United States or in his absence the Acting Attorney General.

(8) "Minimization procedures" means procedures to minimize the acquisition of information that is not foreign intelligence information, to assure that information which is not foreign intelligence information not be maintained, and to assure that information obtained not be used except as provided in Section 2526.

On page 5, line 9, insert the word "publicly" after the word "shall".

On page 5, line 13, strike out the period and insert in lieu thereof a comma and the following:

except that no judge designated under this subsection shall have jurisdiction of an application for electronic surveillance under this chapter which has been denied previously by another judge designated under this subsection. If any judge designated under this subsection denies an application for an order authorizing electronic surveillance under this chapter, such judge shall provide immediately for the record a complete written statement of the reasons for his decision and, on motion of the United States, direct that the record be transmitted, under seal, to the special court of review established in subsection (b).

On page 5, line 14, insert the word "publicly" after the word "shall".

On page 5, line 15, insert the word "publicly" after the word "be".

On page 5, lines 17 through 23, strike out all after the words "special court of" and insert in lieu thereof the following:

review which shall have jurisdiction to review the denial of any application made under this chapter. If such special court determines that the application was properly denied, the special court shall immediately provide for the record a complete written statement of the reasons for its decision and, on motion of the United States, direct that the record be transmitted to the Supreme Court, which shall have jurisdiction to review such decision.

On page 5, line 24, through page 6, line 2, strike out all of subsection "(c)" and insert in lieu thereof the following new subsection:

(c) All proceedings under this chapter shall be conducted as expeditiously as possible. The record of proceedings under this chapter, including applications made and orders granted, shall be sealed by the presiding judge and shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General.

On page 6, line 5, insert the words "by a federal officer" after the word "made".

On page 6, lines 7 and 8, strike out the words "must be approved by the Attorney General" and insert in lieu thereof the words "shall require the approval of the Attorney General based".

On page 6, line 11, insert the word "federal" after the words "of the".

On page 6, line 17, strike out the word "subject" and insert in lieu thereof the word "target".

On page 7, line 4, strike the words "acquisition and retention" and insert in lieu thereof the words "acquisition, retention, and dissemination, and to require the expunging,".

On page 7, lines 8 through 13, strike out all of paragraph (5) after the words "United States" and insert in lieu thereof a colon and the following:

(A) to protect itself against actual or potential attack of other grave hostile acts of a foreign power or an agent of a foreign power;

(B) to provide for the national defense or the security of the Nation;

(C) to provide for the conduct of the foreign affairs of the United States;

(D) to protect against the terrorist activities of a foreign power or an agent of a foreign power;

(E) to protect itself against the sabotage activities of a foreign power or an agent of a foreign power; or

(F) to protect itself against the clandestine intelligence service or network of a foreign power or an agent of a foreign power;

except, that appropriate steps shall be taken to insure that information retained which relates solely to the conduct of foreign affairs shall not be maintained in such a manner as to permit the retrieval of such information by reference to a citizen of the United States who is a party to a communication intercepted as provided in this chapter.

On page 7, lines 14 through 24, strike out all of paragraph "(6)" and insert in lieu thereof the following three new paragraphs:

(6) If the target of the electronic surveillance is a foreign power which qualifies as such solely on the basis that it is an entity controlled and directed by a foreign government or governments, and unles there is probable cause to believe that a substantial number of the officers or executives of such entity are officers or employees of a foreign government, or agents of a foreign power as defined in section 2521(2), (B), (C), (D), or (E), a statement of the procedures to prevent the acquisition, retention, and dissemination and to require the expunging of communications of permanent resident aliens and citizens of the United States who are not officers or executives of such entity responsible for those areas of its activities which involve foreign intelligence information.

(7) a factual description of the nature of the information sought;

(8) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by and with the advice and consent of the Senate—

(A) that the information sought is foreign intelligence information;

(B) that the purpose of the surveillance is to obtain foreign intelligence information;

(C) that such information cannot feasibly be obtained by normal investigative techniques;

(D) including a designation of the type of foreign intelligence information being sought according to the categories described in section 2521(b)(3); and

(E) including a statement of the basis for the certification that—

(i) the information sought is the type of foreign intelligence information designated, and

(ii) such information cannot feasibly be obtained by normal investigative techniques.

On page 8, line 1, strike out the number "(7)" and insert in lieu thereof the number "(9)".

On page 8, line 3, strike out the number "(8)" and insert in lieu thereof the number "(10)".

On page 8, line 4, strike out the words "known to the Attorney General".

On page 8, line 9, strike out the number "(9)" and insert in lieu thereof the number "(11)".

On page 9, line 9, insert the words "made by a federal officer and" after the word "been".

On page 9, lines 20 and 21, strike out the words "acquisition and retention" and insert in lieu thereof the words "acquisition, retention, and dissemination, and to require the expunging,".

On page 9, line 24 through page 10, line 4, strike out all of paragraph (4) after the words "United States" and insert in lieu thereof a colon and the following:

(A) to protect itself against actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) to provide for the national defense or the security of the Nation;

(C) to provide for the conduct of the foreign affairs of the United States;

(D) to protect against the terrorist activities of a foreign power or an agent of a foreign power; or

(F) to protect itself against the clandestine intelligence service or network of a foreign power or an agent of a foreign power;

except, that appropriate steps shall be taken to insure that information retained which relates solely to the conduct of foreign affairs shall not be maintained in such a manner as to permit the retrieval of such information by reference to a citizen of the United States who is a party to a communication intercepted as provided in this chapter.

(5) If the target of the electronic surveillance is a foreign power which qualifies as such solely on the basis that it is an entity controlled and directed by a foreign government or governments, and unless there is probable cause to believe that a substantial number of the officers or executives of such entity are officers or employees of a foreign government, or agents of a foreign power as defined in section 2521(2)(B), (C), (D), or (E), procedures to be followed are reasonably designed to prevent the acquisition, retention, and dissemination, and to require the expunging, of communications of permanent resident aliens and citizens of the United States who are not officers or executives of such entity responsible for those areas of its activities which involve foreign intelligence information.

On page 10, lines 5 through 10, strike all of paragraph "(5)" and insert in lieu thereof the following new paragraph:

(6) the application which has been filed contains the description and certification or certification specified in section 2524(a) (7) and (8).

On page 11, line 23, insert the word "new" after the word "after".

On page 11, line 24, after the period insert the words "In connection with the new findings of probable cause, the judge may require the applicant to submit information obtained pursuant to the original order or to any previous extensions, or any other information or evidence as he finds necessary to make such new findings."

On page 12, line 21, after the period, insert the words "If the Attorney General authorizes such emergency employment of electronic surveillance, he shall require that the minimization procedures required by this chapter for the issuance of a judicial order be followed."

On page 13, line 18, strike out the word "to" and insert in lieu thereof the word "by".

On page 13 line 21 through page 14, line 4, strike out all of subsection "(a)" after the words "United States" and insert in lieu thereafter a colon and the following:

(1) to protect itself against actual or potential attack or other grave hostile acts of a foreign power or agent of a foreign power;

(2) to provide for the national defense or the security of the Nation;

(3) to provide for the conduct of the foreign affairs of the United States;

(4) to protect against the terrorist activities of a foreign power or an agent of a foreign power;

(5) to protect itself against the sabotage activities of a foreign or an agent of a foreign power; or

(6) to protect itself against the clandestine intelligence activities of an intelligence service or network of a foreign power or an agent of a foreign power; or for the enforcement of the criminal law. No otherwise privileged communication obtained in accordance with or in violation of the provisions of this chapter shall lose its privileged character.

On page 14, lines 5 through 8, strike out all of subsection (b) and insert in lieu thereof the following new subsection:

(b) The minimization procedures required under this chapter shall not preclude the retention and disclosure, for law enforcement purposes, of any information which constitutes evidence of a crime if such disclosure is accompanied by a statement that such evidence, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

On page 15, line 6, strike out the word "may" and insert in lieu thereof the word "shall".

On page 15, line 8, strike out the words "only" and "such".

On page 15, lines 9 through 11, strike out all the language and insert in lieu thereof the words "there is a reasonable question as to the legality of the surveillance and that such disclosure would promote a more accurate determination of such legality, or that such disclosure would not harm the national security".

On page 16, lines 12 and 13, strike out the words "and the national security".

On page 17, line 10, insert the letter (a) before the word "In".

On page 17, after line 24, insert the following new subsection:

(b) Nothing in this chapter shall be deemed to limit the authority of the Select Committee on Intelligence of the United States Senate to obtain such information as it may need to cary out its duties pursuant to Senate Resolution 400, 94th Congress, agreed to May 19, 1976.

On page 18, line 10, after the word "have", insert a comma and the words "subject to determination by the courts,".

On page 18, line 14, strike out the number "(2)" and insert in lieu thereof the number "(6)".

On page 18, lines 21 and 22, strike out the words "a reasonable time thereafter, transmit to the" and insert in lieu thereof the words "seventy-two hours of the initiation of such surveillance, transit to the Select Committee on Intelligence of the United States Senate and the".

On page 19, lines 17 and 18, strike out all of subsection "(a)" and insert in lieu thereof the following new subsection:

(a) Section 2511(1) is amended—

(1) by inserting "or chapter 120 or as otherwise authorized by a search warrant or order of a court of competent jurisdiction," immediately after "chapter" in the first sentence;

(2) by inserting a comma and "or, under color of law, willfully engages in any other form of electronic surveillance as defined in chapter 120" immediately before the semicolon in paragraph (a);

(3) by inserting "or information obtained under color of law by any other form of electronic surveillance as defined in chapter 120" immediately after "contents of any wire or oral communication" in paragraph (c);

(4) by inserting "or any other form of electronic surveillance, as defined in chapter 120," immediately before "in violation" in paragraph (c);

(5) by inserting "or information obtained under color of law by any other form of electronic surveillance as defined in chapter 120" immediately after "any wire or oral communication" in paragraph (d); and

(6) by inserting "or any other form of electronic surveillance, as defined in chapter 120," immediately before "in violation" in paragraph (d).

On page 19, line 21 through page 20, line 18, strike out all of subsection "(b)" and insert in lieu thereof the following new subsection:

'(b)(1) Section 2511(2)(a)(i) is amended by inserting the words "or radio communication" after the words "wire communication" and by inserting the words "or otherwise acquire" after the word "intercept".

(2) Section 2511(2)(a)(ii) is amended by inserting the words "or chapter 120" after the second appearance of the word "chapter", and by striking the period at the end thereof and adding the following: "or engage in electronic surveillance, as defined in chapter 120: *Provided, however*, That before the information, facilities, or technical assistance may be provided, the investigative or law enforcement officer shall furnish to the officer, employee, or agency of the carrier either—

(1) an order signed by the authorizing judge certifying that a court order directing such assistance has been issued, or

(2) in the case of an emergency surveillance as provided for in section 2518(7) of this chapter or section 2525(d) of chapter 120, or a surveillance conducted under the provisions of section 2528 of chapter 120, a sworn statement by the investigative or law enforcement officer certifying that the applicable statutory requirements have been met,

and setting forth the period of time for which the surveillance is authorized and describing the facilities from which the communication is to be intercepted. Any violation of this subsection by a communication common carrier or an officer, employee, or agency thereof, shall render the carrier liable for the civil damages provided for in section 2520.

On page 20, line 19 through page 21, line 12, strike out all of subsection "(c)" and insert in lieu thereof the following new subsection:

(c)(1) Section 2511(2)(b) is amended by inserting the words "or otherwise engage in electronic surveillance, as defined in chapter 120," after the word "radio".

(2) Section 2511(2)(c) is amended by inserting the words "or engage in electronic surveillance, as defined in chapter 120," after the words "oral communication" and by inserting the words "or such surveillance" after the last word in the paragraph and before the period.

(3) Section 2511(2) is amended by adding at the end of the section the following provision:

(e) It shall not be unlawful under this chapter or chapter 120, or section 605 of the Commissions Act of 1934 for an officer, employee, or agent of the United States in the normal course of his official duty, to conduct electronic surveillance as defined in section 2521(b)(2) of chapter 120, for the sole purpose of determining the capability of equipment used to obtain foreign intelligence or the existence or capability of equipment used by a foreign power or its agents: *Provided*, (1) That the test period shall be limited in extent and duration to that necessary to determine the capability of the equipment, and (2) that the content of any communication acquired under this section shall be retained and used only for the purpose of determining the existence or capability of such equipment, shall be disclosed only to the officers conducting the tset or search, and shall be destroyed upon completion of the testing or search period; and (3) that the test may exceed ninety days only with the prior approval of the Attorney General.

On page 21, lines 14 and 15, strike out all of subsection "(e)" and insert in lieu thereof the following new subsection:

(e) Section 2515 is amended by inserting the words "or electronic surveillance as defined in chapter 120, has been made" after the words "intercepted" and by inserting the words "or other information obtained from electronic surveillance, as defined in chapter 120," after the second appearance of the word "communication".

On page 22, lines 6 through 12, strike out all of subsection "(k)" and insert in lieu thereof the following new subsection:

(k) Section 2520 is amended by deleting all before subsection (2) and inserting in lieu thereof:

Any person other than an agent of a foreign power as defined in section 2521(b)(2)(A) of chapter 120, who has been subject to electronic surveillance, as defined in chapter 120, or whose wire or oral communication has been intercepted, or about whom information has been disclosed or used, in violation of this chapter, shall (1) have a civil cause of action against any person who so acted in violation of this chapter and.

On page 22, after line 12, insert the following new sections:

SEC. 5. On or before March 1, 1978, and on the first day of March of each year thereafter, the Select Committee on Intelligence of the United States Senate shall report to the Senate concerning the implementation of this chapter. Said reports shall include but not be limited to an analysis and recommendations concerning whether this chapter should (1) be amended, (2) repealed, or (3) permitted to continue in effect without amendment.

SEC. 6. (a) In the event the Select Committee on Intelligence of the United States Senate shall report that this chapter should be amended or repealed, it shall report out legislation embodying its recommendations within thirty calendar days, unless the Senate shall otherwise determine by yeas and nays.

(b) Any legislation so reported shall become the pending business of the Senate with time for debate equally divided between the proponents and the opponents and shall be voted on within three calendar days thereafter, unless the Senate shall otherwise determine by yeas and nays.

(c) Such legislation passed by the Senate shall be referred to the appropriate committee of the other House and shall be reported out by such committee together with its recommendations within thirty calendar days and shall thereupon become the pending business of such House and shall be voted upon within three calendar days, unless such House shall otherwise determine by yeas and nays.

(d) In the case of any disagreement between the two Houses of Congress with respect to such legislation passed by both Houses, conferees shall be promptly appointed and the committee of conference shall make and file a report with respect to such legislation within seven calendar days after the legislation is referred to the committee of conference. Notwithstanding any rule in either House concerning the printing of conference reports in the record or concerning any delay in the consideration of such reports, such report shall be acted on by both Houses not later than seven calendar days after the conference report is filed. In the event the conferees are unable to agree within three calendar days they shall report back to their respective Houses in disagreement.

History of the Bill

The Foreign Intelligence Surveillance Act of 1976, S. 3197, was introduced by Senator Kennedy on March 23, 1976. It was cosponsored by seven other Senators: Mr. Nelson, Mr. Mathias, Mr. Hugh Scott, Mr. McClellan, Mr. Hruska, Mr. Bayh, and Mr. Robert C. Byrd. The bill was referred at that time to the Committee on the Judiciary.

The Subcommittee on Criminal Laws and Procedures, chaired by Senator McClellan, held hearings on the bill on March 29 and 30. The subcommittee amended the bill in several respects and ordered a favorable report. Subsequently, on June 15, the subcommittee amendment by substitution was considered and ordered reported favorably by the Judiciary Committee.

On June 16, Senator Inouye, the Chairman of the Select Committee on Intelligence, requested referral of S. 3197 to that Committee, pursuant to the provisions of S. Res. 400, 94th Congress, 2nd Session. The bill was ordered referred to the Select Committee upon its discharge from the Committee on the Judiciary.

The Subcommittee on Intelligence and the Rights of Americans held hearings on S. 3197 on June 29, 30, and July 1. The hearings included one day of testimony in executive session on the needs of the intelligence community for electronic surveillance information.

The subcommittee adopted a number of amendments in response to testimony received in the course of its hearings. A favorable report was ordered on August 6.

The subcommittee amendments and some additional amendments were adopted by the full Select Committee on Intelligence, which on August 10 ordered S. 3197 as amended favorably reported by a vote of 14 ayes and 1 nay, as follows:

YEAS	NAYS
Mr. Inouye	Mr. Morgan
Mr. Baker	
Mr. Bayh	
Mr. Stevenson	
Mr. Hathaway	
Mr. Huddleston	
Mr. Biden	
Mr. Hart	
Mr. Case	
Mr. Thurmond	
Mr. Hatfield	
Mr. Goldwater	
Mr. Stafford	
Mr. Garn	

Purpose of the Select Committee's Amendments

The Committee on the Judiciary adopted a number of amendments to S. 3197 for the purpose of clarifying statutory intent and providing safeguards for the individuals subjected to electronic surveillance. The purpose of the amendments of the Committee on Intelligence has been to further clarify legislative intent, particularly with respect to those circumstances where electronic surveillance of Americans for foreign

intelligence purposes may be authorized. Procedures for obtaining foreign intelligence surveillance warrants are described in additional detail. An effort has also been made to strengthen protection against abuses involving information received through such surveillance. Finally, further conforming amendments have been made to Chapter 119 of Title 18, United States Code (Title III of the Omnibus Crime Control and Safe Streets Act of 1968, P.L. 90–135, section 802).

Position of the Administration

The Department of Justice has supported the enactment of S. 3197 from its introduction. As the Attorney General testified before the Subcommittee on Intelligence and the Rights of Americans on July 1, 1976:

> Enactment of the bill will, I believe, provide major assurance to the public that electronic surveillance will be used in the United States for foreign intelligence purposes pursuant to carefully drawn legislative standards and procedures. The bill ensures accountability for official action. It compels the Executive to scrutinize such action at regular intervals. And it requires independent review at a critical point by a detached and neutral magistrate.
>
> In providing statutory standards and procedures to govern the use of electronic surveillance for foreign intelligence purposes in this country and in establishing critical safeguards to protect individual rights, the bill also ensures that the President will be able to obtain information essential to protection of the Nation against foreign threats. While guarding against abuses in the future, it succeeds, I trust, in avoiding the kind of reaction against abuses of the past that focuses solely on these abuses, but is careless of other compelling interests.

The Select Committee has worked closely with representatives of the Department of Justice and with members of the Judiciary Committee, consistent with the mandate of S. Res. 400, Section 3, in drafting amendments to clarify the language of S. 3197. It has been the purpose of both the Committee and the Department to provide maximum protection for the civil liberties of persons who may be subject to surveillance under this Act, while maintaining the capability of the United States to obtain necessary foreign intelligence by electronic means. The bill as amended receives the Administration's continued support.

General Statement

I. SUMMARY OF THE LEGISLATION

S. 3197 amends Title 18, United States Code, by adding a new chapter after chapter 119, entitled "Electronic Surveillance Within the United States for Foreign Intelligence Purposes." The bill requires a warrant for any electronic surveillance conducted for foreign intelligence purposes of law enforcement. The combined effects of chapter 119 and this new chapter, if enacted, would be to require a warrant for any electronic surveillance conducted within the United States.

S. 3197 does not, however, require a warrant for electronic surveillance abroad, including some surveillance of communications in which one party may be located within the United States. The bill in no way authorizes warrantless wiretaps anywhere for any purpose. However, any constitutional power which the courts determine that the President has, independent of statutory authority, to conduct warrantless wiretaps abroad or for emergency purposes in unforeseen circumstances, if such power exists, is expressly limited in that it can only be exercised in the circumstances enunciated in subsections (a) and (b) of Section 2528.

The bill provides a procedure by which the Attorney General, upon the general authorization of the President to conduct electronic surveillance within the United States for foreign intelligence purposes, may authorize applications to the courts for warrants to conduct such surveillance. Applications for warrants are to be made to one of seven district court judges publicly designated by the Chief Justice of the Supreme Court. Denials of such applications may be appealed to a special three-judge court of review and ultimately to the Supreme Court.

Approval of a warrant application under this bill would require a finding by the court that the target of the surveillance is a "foreign power" or an "agent of a foreign power." A "foreign power" may include a foreign government, a faction of a foreign government, a foreign political party, a foreign-based terrorist group, or an entity directed and controlled by a foreign government. An "agent of a foreign power" includes foreigners who are officers or employees of a foreign power as well as some American citizens or permanent resident aliens who act on behalf of a foreign power. The court would be required to find that the facilities or place at which the electronic surveillance is to be directed are being used or are about to be used by a foreign power or an agent of a foreign power.

Approval of the warrant would also require a finding that procedures will be followed in the course of the surveillance to minimize the acquisition, retention, and dissemination, and to require the expunging of information relating to permanent resident aliens or citizens of the United States which does not relate to national defense, foreign affairs, or the terrorist activities, sabotage activities, or clandestine intelligence activities of a foreign power. Special minimization procedures for electronc surveillance directed at entities directed and controlled by foreign governments which are largely staffed by Americans are also subject to judicial review.

Finally, the court would be required to find that a certification or certifications have been made by the Assistant to the President for National Security Affairs or executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate. Such official or officials would be required to certify that the information sought by the surveillance requested is information essential to the national defense or the conduct of foreign affairs of the United States or is necessary to the ability of the United States to protect itself against the clandestine intelligence, terrorist, or sabotage activities of a foreign power. The court would not be required to find that the information

sought is in fact information of the type described in the certification, but that a detailed written certification to that effect has been made by the appropriate official or officials.

The court could approve electronic surveillance for foreign intelligence purposes for a period of ninety days. Any extension of the surveillance beyond that period would require a reapplication to the court and new findings as required for the original order.

Emergency warrantless surveillances would be permitted in limited circumstances, provided that a warrant is obtained within twenty-four hours of the initiation of the surveillance.

For purposes of oversight, S. 3197 requires annual reports to the Administrative Office of the United States Courts and the Congress of various statistics related to applications and warrants for electronic surveillance, as well as an annual detailed report by the Select Committee concerning whether the law should be changed, repealed, or allowed to remain in effect. The Select Committee on Intelligence has added a provision that nothing in the bill shall be deemed to restrict the authority of the Select Committee to obtain further information related to its oversight responsibilities pursuant to S. Res. 400, 94th Congress, 2nd Session.

Statement of Need for Legislation

The purpose of the Foreign Intelligence Surveillance Act of 1976 is to require a judicial warrant and to provide for legislative review of all electronic surveillance conducted for reasons of national security. It has long been recognized that national security wiretaps, exempted from the warrant provisions of the Omnibus Crime Bill of 1968, could be subject to abuse. Recent investigations by the Senate Select Committee on Governmental Operations with Respect to Intelligence Activities provided firm evidence that national security wiretaps were abused and that checks upon the exercise of these clandestine methods were clearly necessary.

The basic premise of the bill is that a warrant for national security wiretaps can be devised which is consistent with the "reasonable search" requirements of the fourth amendment. The Committee found that national security wiretaps are justified in cases of espionage, sabotage, and counter-terrorism. Far more troublesome questions arose as to whether electronic surveillance is justified to gather economic intelligence or information related to, or deemed essential to, the conduct of foreign affairs. The Committee found that such surveillance was justified in certain limited circumstances to protect the security of the United States. Because of the breadth of the authorization required for such surveillance, each such surveillance must be the subject of a judicial warrant procedure and must be subject to the strictest review by the legislative branches.

Troublesome questions also arose as to whether electronic surveillance of United States citizens and permanent resident aliens should be permitted in circumstances where probable cause to believe that there has been or is about to be a violation of the criminal law could not be shown. The Committee has reviewed data on a variety of circumstances where it is not possible to meet a probable cause test, but where reasonable men would agree that information essential to the

national security can be obtained only through electronic surveillance. The Committee has only begun to examine the possibility of resolving this problem through expanding the criminal law in the intelligence area. The Committee is impressed, however, with the difficulty of drafting constitutionally acceptable language which is sufficiently broad to bring all intelligence activities of which the United States needs to be aware within the ambit of the criminal law. Although it might be possible to revise the criminal law, the difficulties experienced in other countries with "official secrets acts" are symptomatic of the problems. Thus, the Committee has reluctantly agreed to authorize national security electronic surveillance in the absence of probable cause to believe that a crime has been or is about to be committed.

While the Committee recognizes the requirements of the United States for intelligence which can be obtainetd only through electronic surveillance, we are also aware of the dangers that such surveillance poses to individual liberties. Such electronic surveillance should be conducted only through carefully defined procedures, with well-defined lines of authority within the Executive branch. Finally, the Committee is deeply committed to the view that this highly intrusive investigative technique must be subject to judicial review and congressional oversight.

In the absence of legislation such as S. 3197, the United States is left with two options: To abandon electronic surveillance for any purpose other than law enforcement, and thus risk the loss of intelligence of importance to the security of the United States, or to engage in such surveillance in the absence of legislative guidelines and judicial or congressional review.

In the view of the Committee, neither option is acceptable. To meet the need posed, S. 3197 provides for constitutional checks designed to determine whether there is a necessity for a particular electronic surveillance and proper execution of a warranted "reasonable search." The means used is the proper involvement of all three branches in their appropriate ways. Its main feature is that warrants for national security wiretaps are not solely within the discretion of the Executive branch but must be reviewed by the courts. Further, they are subject to oversight by the Legislative branch. Under the bill, no national security electronic surveillance in the United States, as defined in the bill, can take place without a judicial warrant. Further, the full details of all warranted electronic surveillance are subject to legislative oversight.

Even though questions remain whether further criminal statutes might be desirable to cover areas now in the amorphous national security area, the procedure provided by the bill is a great advance over the existing legal situation in which national security wiretaps lie outside of constitutional review by the courts or the Legislature.

Section-by-Section Analysis

Section 1 of the bill provides that the Act may be cited as the "Foreign Intelligence Surveillance Act of 1976."

Section 2 of the bill amends the Omnibus Crime Control and Safe Streets Act of 1968 (Pub. L. 90–351, Title III, section 802) by adding a new chapter 120 and items 2521–2528:

Section 2521

Subsection (a) provides that except for those terms specifically defined in this section the definitions of chapter 119, relating to the interception of wire and oral communications, apply to this chapter as well.

Subsection (b)(1) defines "foreign power" in five separate ways:

(A) "A foreign government or any component thereof, whether or not recognized by the United States." This category would include foreign governmental establishments which are located in the United States.[1]

(B) "A faction of a foreign nation or nations, not substantially composed of permanent resident aliens or citizens of the United States." This category is intended to include factions of a foreign nation or nations which are in a contest for power over, or control of the territory of, a foreign nation or nations. The faction must be foreign-based and controlled from abroad. Specifically excluded from this category is any faction of a foreign government or government which is substantially composed of permanent resident aliens or citizens of the United States.

(C) "An entity, which is directed and controlled by a foreign government or governments." This category is intended to include two types of entity: (i) An entity which appears to be a legitimate foreign commercial establishment, but which is being utilized by a foreign government as a cover for espionage activities; and (ii) a legitimate foreign commercial establishment which is directed and controlled by a foreign government and which, because of the nature of its operations, constitutes an essential source of valuable foreign intelligence information which would otherwise be unavailable to the U.S. Government.

The Committee is concerned about the realistic possibility that many wholly innocent permanent resident aliens or citizens of the United States might be employed by such entities, and that their rooms and telephones could be subject to surveillance under this category. The Committee would have preferred to have required that any such entity to be surveilled not be substantially composed of permanent resident aliens or citizens of the United States. If such a requirement were to have been included in the bill, those entities which were established as "covers" for espionage would have needed only to hire a number of Americans in order to avoid electronic coverage. Accordingly, such a requirement has not been included. In order to provide adequate protection for innocent Americans, however, the Committee has included a "minimization" requirement, see Section 2524(a)(6), *infra*, to insure that the conversations of such persons are not surveilled.

A law firm in the United States which represents a foreign government or an interest of a foreign government is not by such representation "an entity, which is directed and controlled by a foreign government or governments."

(D) "A foreign-based terrorist group." This category means a foreign-based group whose primary activities involve "terrorist activities" as defined elsewhere in the bill. (See subsection (b)(3), *infra*).

[1] This bill is not intended, of course, to repeal or abrogate the Vienna Convention on Diplomatic Relations, which was ratified by the Senate and came into effect in the United States on December 13, 1972.

The category does not include a group of American citizens or permanent resident aliens who are living or headquartered abroad.

(E) "A foreign-based political organization, not substantially composed of permanent resident aliens or citizens of the United States." This category is intended to include those foreign political parties which are mere instrumentalities of a foreign government and which are not substantially composed of Americans. This category is not intended to include political parties which are not directed and controlled by a foreign country, and clearly does not include organizations comprised of Americans of Greek, Irish, Jewish, Chinese or other extraction, who have joined together out of interest in or concern for the country of their ethnic origin.

Subsection (b)(1) defines an "agent of a foreign power" in two separate ways. Subparagraph (A) includes officers or employees of foreign powers who are not United States citizens or aliens lawfully admitted for permanent resident. The definition is framed in this way because it is presumed that nonresident aliens who are officers or employees of a foreign power are likely sources of foreign intelligence information. Employees of a foreign power are meant to include those persons who have a normal employee-employer relationship. The subparagraph is not intended to encompass such foreign visitors as professors, lecturers, exchange students, performers, or athletes, even if they are receiving remuneration or expenses from their home government in such capacity.

Subparagraphs (B), (C) and (D) of subsection (b)(1) comprise the second definition of "agent of a foreign power." They define the agent in terms of the activities in which he is engaged for or on behalf of a foreign power.

Subparagraphs (B) (i) and (ii), and (C) (i) and (ii) encompass any person who is (i) knowingly engaged in terrorist or sabotage activities for or on behalf of a foreign power, or who (ii) consciously conspires with, aids, or abets such a person, with knowledge of what that person is doing and for whom he is doing it. "Terrorist activities" and "sabotage activities" are defined elsewhere in the bill and must be criminal in nature. (See subparagraphs (b)(3) and (b)(4) *infra*).

Under subparagraph (B)(i) and (C)(i) the person to be surveilled must be shown to have a knowing and substantial connection with the foreign power for whom he is working. In the case of terrorist activities, it is anticipated that in most cases that connection will be shown to exist with a "foreign-based terrorist group." In no event may mere sympathy for, or identity of interest with, the goals of a foreign group or government be sufficient. The person to be surveilled must be clearly and knowingly acting for or on behalf of the foreign power itself, in a principal-agent relationship. The Committee intends that this bill not authorize electronic surveillance under any circumstances for the class of individuals included by the Supreme Court within the scope of the *Keith* decision requiring judicial warrants for alleged threats to security of a purely domestic nature.

The same knowing and substantial connection with a foreign power must likewise be found to exist with respect to the person who is knowingly acting "in furtherance of" terrorist or sabotage activities. The "in furtherance of" phrase is in no way intended to dilute the requirements of knowledge, active engagement in the activities, or the

requisite connection and agency relationship with the foreign power, and has been included only in order to permit electronic coverage at some point prior to the moment when the danger sought to be prevented, e.g., a kidnapping, bombing, or hijacking, actually occurs.

Subparagraphs (B) (ii) and (C) (ii) encompass those persons who consciously conspire with, aid, or abet a person who is knowingly engaged in terrorist or sabotage activities for or on behalf of a foreign power. In order to target electronic surveillance against someone who is not himself engaging in terrorist or sabotage activities for a foreign power, but who is allegedly conspiring with or aiding and abetting a person engaged in such activities for a foreign power, the Government would have to establish probable cause that the prospective target knew both that the person with whom he was conspiring or whom he was aiding or abetting was engaging in such activities as an agent of a foreign power and that his own conduct was assisting or furthering such activity. The knowledge requirement is therefore applicable to both the status of the person being aided by the subject of the surveillance and the nature of the activity being promoted.

In the case of a person alleged to be knowingly aiding or abetting those engaged in terrorist activities for a foreign power, such a person might be assisting a group which is engaged in both lawful political activity and unlawful terrorist acts. In such a case, it would be necessary to establish probable cause that the individual was aware of the terrorist activities undertaken by the group and was knowingly furthering them, and not merely that he was aware of and furthering their lawful activity.

Subparagraphs (D) (i) and (ii), and (E), encompass the third category of activities (other than terrorism and sabotage) for which any person (foreigner, citizen, or permanent resident alien) who has a substantial connection with a foreign power may be subjected to electronic surveillance under this bill. This is the category which involves clandestine intelligence activities. This category includes three classes of people:

Subparagraph (D) (i) is intended to include those persons who are knowingly acting for or on behalf of a foreign power and are knowingly engaged in clandestine intelligence activities in violation of federal criminal law. Once again, as was the case with respect to persons engaged in terrorist or sabotage activities (subparagraphs (B) (i) and (C) (i)), the person to be surveilled must be demonstrated to have a knowing and substantial connection with a foreign power. The Committee wishes to stress that this bill is not intended to authorize electronic surveillance under any circumstances for the class of individuals included by the Supreme Court within the scope of the *Keith* decision requiring judicial warrants for alleged threats to security of a purely domestic nature. In short, under this subparagraph, the person to be surveilled must be clearly and knowingly acting for or on behalf of a foreign power itself. There must be a principal-agent relationship under which the alleged agent has undertaken to do the bidding of his foreign principal. Or, as described by the Attorney General in his testimony before the Committee, the agent must be shown to have achieved the status of "a secret agent who operates as part of the foreign intelligence service of a foreign power."[2]

[2] Hearings, p. ——, July 1, 1976.

Under this subparagraph, the agent must be knowingly engaged in "clandestine intelligence activities" which violate or will violate federal criminal law. It is anticipated that most of the persons surveilled will be violating the criminal espionage laws which appear in title 18, U.S. Code, sections 792–799, 951 (see e.g., *Abel* v. *U.S.*, 362 U.S. 217) ; title 42, U.S. Code, sections 2272–2278b; and title 50, U.S. Code, section 855, for the term "clandestine intelligence activities" is directed primarily toward those traditional activities associated with "spying." In addition to the activities which fall within the substantive statutory definition of spying are activities directly related to spying which may constitute violations of laws which proscribe the aiding and abetting of spying, such as maintaining a "safehouse" for secret meetings, servicing "letter drops" to facilitate covert transmission of instructions or information, recruiting new agents, or infiltrating and exfiltrating agents under deep cover to and from the United States.

Apart from the types of activities specifically proscribed by the espionage laws, the bill is intended to permit the surveillance of foreign intelligence agents who are collecting industrial or technological information which, if disclosed to a hostile foreign power, would present a significant threat to the security of the nation. In such a case, the Government would have to establish that the agent was collecting or transmitting such information in a manner which would constitute a violation of some other federal statute, such as title 18, U.S. Code, section 2514, which proscribes the interstate transportation of stolen property. It also seems clear that in some cases the knowing transfer of technological information to a foreign country without a license from the federal government would be unlawful under the "Export Administration Act" (Title 50, U.S. Code, sections 2021–2032).

However, clandestine collection of information regarding the business plans or trade secrets of an American company which merely might provide a competitive advantage to foreign firms, for example, in bidding on a contract with a third country—even if such collection violated a federal criminal statute—would not be "clandestine intelligence activity".

In addition to conventional "spying," that is, the gathering of information, the intelligence agencies of foreign powers also engage in covert action designed to influence events in this country. Under this subparagraph, however, only if such covert political action involves a violation of federal criminal law, such as Title 18, U.S. Code, section 201 (bribery of public officials) and is undertaken directly on behalf of a foreign power, would it be encompassed by this subparagraph.

The bill does not authorize electronic surveillance when the activities, even though secret and conducted for a foreign power, involve lawful acts such as lobbying. And clearly excluded is any activity which involves the lawful exercise of first amendment rights of speech, petition, assembly, and association. In no event may political activity within the ambit of the protections afforded by the first amendment be the basis, or form any part of the basis, for finding that an American citizen or permanent resident alien is engaged in "clandestine intelligence activities."

Thus, failing to comply fully with the Foreign Agents Registration Act (22 U.S.C. 611, *et seq.*) in and of itself is not intended to be

clandestine merely because the agent seeks to lobby Congress or influence public opinion on matters relating to the national defense or foreign affairs. Americans exercising their right to lobby public officials or to engage in organized political dissent from official policy may well be in contact with representatives of foreign governments and groups when the issues concern foreign affairs or international economic matters. In the future, Americans must continue to be free to communicate, about such issues and to obtain information or exchange views with representatives of foreign governments or with foreign groups, free from any fear that such contact might be a basis to find probable cause they are acting at the direction of a foreign power, thus triggering the Government's power to conduct electronic surveillance.

The word "involve" as used in this subparagraph is not intended to encompass any individuals who are not actually engaged in a violation of federal law. It is intended to encompass a violation of federal law which is an integral part of the clandestine intelligence activity. The phrase "will involve" which also appears in this subparagraph is likewise in no way intended to diminish or dilute the nature of the criminal activity to be established. The only purpose of its inclusion is in order to permit electronic coverage at some point prior to the time when the actual crime sought to be prevented, for example the actual passage of classified documents, actually occurs. The Committee recognizes that under this explanation an argument might be made that a person could be surveilled for an inordinate period of time. That is not the intention. And indeed, even upon an assertion by the government that an informant has claimed that someone has been instructed by a foreign power to go into "deep cover" for several years before actually commencing his espionage activities, such facts would not necessarily be encompassed by the phrase "will involve." Indeed, under the extension provisions of section 2525(c), discussed in greater detail infra, the judge can insist on examining the fruits of any earlier surveillance to determine whether he continues to be satisfied that there is probable cause to believe that the individual will be involved in clandestine intelligence activities.

Subparagraph (D)(ii) encompasses those persons who consciously conspire with, aid, or abet a person who is knowingly engaged in criminal clandestine intelligence activities for a foreign power. In order to target electronic surveillance against someone who is not himself engaging in such activities for a foreign power, but who is allegedly conspiring with or aiding and abetting a person engaged in such activities for a foreign power, the Government would have to establish probable cause that the prospective target knew both that the person with whom he was conspiring or whom he was aiding and abetting was engaged in such clandestine intelligence activities as an agent of a foreign power and that his own conduct was assisting or furthering such activity. The knowledge requirement is therefore applicable to both the status of the person being aided by the subject of the surveillance and the nature of the activity being promoted.

An illustration of the "knowing" requirement is provided by the case of Dr. Martin Luther King. Dr. King was subjected to electronic surveillance on "national security grounds" when he continued to associate with two advisers whom the Government had apprised him

were suspected of being American Communist party members and, by implication, agents of a foreign power. Dr. King's mere continued association and consultation with those advisers, despite the Government's warnings, would clearly not have been a sufficient basis under this bill to target Dr. King as the subject of electronic surveillance.

Indeed, even if there had been probable cause to believe that the advisers alleged to be Communists were engaged in criminal clandestine intelligence activity for a foreign power within the meaning of this section, and even if there were probable cause to believe Dr. King was aware they were acting for a foreign power, it would also have been necessary under this bill to establish probable cause that Dr. King was knowingly engaged in furthering his advisers' criminal clandestine intelligence activities. Absent one or more of these required showings, King could not have been found to be one who knowingly aids or abets a foreign agent.[3]

Subparagraph (E) encompasses the third class of "targetable" persons who are involved in clandestine intelligence activities. This subparagraph reflects the only situation in which a permanent resident alien or citizen of the United States may be surveilled even though the Government cannot establish that he is involved in specific criminal activity. It is the Committee's judgment, however, that this subparagraph contains standards sufficiently stringent so as to afford an extremely high standard of protection consistent with Fourth Amendment requirements. The Committee has also concluded that this restrictive class of "targetable" persons is essential to Government's ability to protect itself against the clandestine intelligence activities of a hostile foreign intelligence service.

This subparagraph is necessary in order to permit the Government to adequately investigate cases such as those where federal agents have witnessed a series of "meets" or "drops" between a hostile foreign intelligence officer and a citizen who might have access to highly classified or other similarly sensitive information; information is being passed, but the federal agents have been unable to determine precisely what information is being transmitted. Such a lack of knowledge would of course disable the government from establishing precisely what crime was being committed. Nevertheless, the Committee believes that in some such cases the circumstances might be such as to make it a potentially extremely dangerous situation which could result in significant harm to the security of the Nation. Accordingly the bill permits, through this subparagraph, the surveillance of the citizen involved if the Government can establish that there is probable cause to believe that he was:

(1) Acting pursuant to the direction of a foreign intelligence service;

[3] Mere membership in the United States Community party is not today sufficient under this bill to establish probable cause that a person is acting for a foreign power or that he is engaged in criminal clandestine intelligence activities.

Moreover, even if additional information established probable cause to believe some members of the party were acting for a foreign power, neither efforts to collect information about the plans and program of the civil rights movement or other political protests, nor efforts to stimulate or shape them would constitute criminal clandestine intelligence activity within this section. Gathering information about the movement would neither be criminal espionage nor involve economic or technical information relating to the national security. Similarly, since the civil rights protest movement itself involved constitutionally protected rights of association, speech and petition for redress of grievances, efforts by a foreign power to involve itself in such a movement are intended to be specifically excluded from any interpretation of clandestine intelligence activity.

(2) Transmitting information to the foreign intelligence service in a manner intended to conceal either the nature of the information being transmitted or the fact that it was being transmitted; and

(3) Transmitting the information under circumstances which would lead a reasonable man to believe that the information will be used to harm the security of the United States, or that lack of knowledge by the United States government about what is being transmitted will harm the security of the United States.

In applying the "reasonable man" test, the judge is expected to take all the known circumstances into account, e.g., who the American is, where he is employed, whether he has access to classified or other sensitive information, the nature of the clandestine meetings (e.g., whether it is merely in an out-of-the-way restaurant, as opposed to a hidden location in a distant city), the method of transmission (e.g., handing over a sealed envelope in a public place, as opposed to using a "drop"), and whether there are any other reasonable explanations for the behavior. It is clear, moreover, that the circumstances must not merely be suspicious, but must be of such a nature as to lead a reasonable man to conclude that the information being transmitted will be used to harm the security of the United States.

This subparagraph also recognizes that there are also certain rare situations where, for example, a citizen who has access to classified information is clandestinely meeting with a known intelligence officer of a hostile foreign power, and it is therefore essential that the United States find out what is transpiring between them because a lack of knowledge by the U.S. Government about what is being transmitted will harm the security of the United States. In such a situation, if the judge concludes that a reasonable man would conclude that such lack of knowledge "will harm the security of the United States," an American might also be targetable.

Subsection (b)(3) defines "terrorist activities" as activities which are criminal, and violent or dangerous to human life. The purpose of the activities must be either the forceful intimidation of a substantial portion of the civilian population or the intimidation of national leaders in order to force a significant change in governmental policy. Examples of such activities would be the detonation of bombs in a metropolitan area, the kidnapping of a high-ranking government official or the hijacking of an airplane in a deliberate and articulated effort to force the government to release a certain class of prisoners or to suspend aid to a particular foreign country.

Subsection (b)(4) defines "sabotage activities" as activities which constitute crimes punishable under chapter 105 of title 18, U.S. Code.

Subsection (b)(5) defines "foreign intelligence information" to include five types of information, which, while not mutually exclusive, tend to be distinguishable. Subparagraph (A) of this subsection is defined as information deemed necessary for the United States to protect itself against actual or potential attack or other similarly grave hostile acts of a foreign power or its agents. This category is intended to encompass information concerning foreign military capabilities and intentions as well as grave acts of force or aggression which would have serious adverse consequences to the national security of the United States. The term "hostile acts" must be read in the context of the sub-

paragraph which is keyed to actual or potential attack on the United States. The Attorney General has testified that "it is the actual or potential attack which really gives flavor to what is meant." [4] Thus, only the most "grave" types of "hostile acts" would be envisioned as falling within this provision.

Subparagraph (B) of this subsection includes information which because of its importance is deemed essential (i) to the national defense or the security of the Nation or (ii) to the conduct of the foreign affairs of the United States. This subparagraph also requires that the information sought involve "information with respect to foreign powers or territories", and would therefore not include information about the views or planned statements or activities of Members of Congress, executive branch officials or private citizens concerning the foreign affairs of the United States.

It is anticipated that the types of "foreign intelligence information" defined in subparagraphs (A) and (B) will be the type sought when an electronic surveillance is instituted upon the type of foreign power defined in Section 2521(b)(1)(A), (B), (C), and (E), or upon most of the foreign agents defined under Section 2521(b)(2)(A).

Subparagraph (c) of this subsection includes information which is deemed necessary for the United States to protect against the terrorist activities of a foreign power or foreign agent. It is anticipated that the type of information described in this subparagraph will be the type sought when an electronic surveillance is instituted upon the type of foreign power defined in Section 2521(b)(1)(D), or upon the type of foreign agent defined in Section 2521(b)(2)(i) and (ii).

Subparagraph (D) of this subsection includes information which is deemed necessary for the United States to protect itself against the sabotage activities of a foreign power or foreign agent. It is anticipated that the type of information described in this subparagraph will be the type sought when an electronic surveillance is instituted upon the type of foreign power defined in Section 2521(b)(1)(A), or upon the type of foreign agent defined in Section 2521(b)(2)(A) and (C).

Subparagraph (E) of this subsection includes information which is deemed necessary to the ability of the United States to protect itself against the clandestine intelligence activities of an intelligence service or network of a foreign power or foreign agent. It is anticipated that the type of information described in this subparagraph will be the type sought when an electronic surveillance is instituted upon the type of foreign power defined in Section 2521(b)(i)(A) or (C), or upon the type of foreign agent defined in Section 2521(b)(2)(A) or (D). This subparagraph encompasses classic counterintelligence information; that is, information deemed necessary to our ability to discover and protect the Nation against the activities of clandestine intelligence services of foreign powers which are directed against the security of the Nation. This subsection is not intended to encompass information sought about dissident political activity by Americans alleged "necessary" to determine the nature and extent of any possible involvement in those activities by the intelligence services of foreign powers. Such a dragnet approach to counterintelligence has

[4] House hearings, pp. 10–11, June 2, 1976.

been the basis for past improper investigations of Americans and is not intended to be included as a permissible avenue of "foreign intelligence" collection under this subparagraph. Nor does this subparagraph include efforts to prevent "news leaks" or to prevent publication of such leaked information in the American press, unless there is reason to believe that such publication is itself being done by an agent of a foreign intelligence service and that such publication would adversely affect the national security.

The "necessary" standard found in subdefinitions (A), (C), (D), and (E) is intended to require more than a mere showing by the government that the information would be significant or useful. It is often contended that the intelligence analyst, if not the policy-maker himself, must have every possible bit of information about a subject because it might prove an important piece of the larger picture. In that sense, any information relating to the specified purposes might be called "necessary" but such a reading is clearly not intended. Rather, the term "necessary" is intended to insure that only the most important information defined in subdivisions (A), (C), (D), and (E) will be acquired pursuant to this chapter.

"Essential" is used in subparagraph (B) because of the more amorphous nature of the information which can be acquired under this subparagraph. While subparagraph (A) deals with positive foreign intelligence involving actual or potential attack or comparable hostile acts and subparagraphs (C), (D), and (E) cover terrorist, sabotage and counterintelligence information, subparagraph (B) potentially brings within the definition of foreign intelligence information a broader range of material dealing with the national defense and foreign affairs of the United States. Therefore, the information sought must be deemed "essential."

The Committee has also made clear by amendment of the "foreign intelligence information" definition, that in no event will information about a United States citizen's private affairs be deemed "foreign intelligence information" unless it directly relates to his activities on behalf of a foreign power. This has been achieved by including in each subsection of the foreign intelligence definition an additional requirement that the information sought actually "relates to" the type of information deemed necessary or essential. For example, the government could not seek purely private life information about a United States citizen or permanent resident alien, who is a suspected spy, upon a theory that they might learn something which would be "compromising." Instead, the bill, as amended, makes clear that the only information about U.S. citizens or permanent resident aliens which may be sought must not only be necessary to the ability of the U.S. to protect itself against clandestine intelligence activities, but must also "relate to" the activities themselves. This restriction might not always be fully applicable to agents of foreign powers as defined in Section 2521(b)(2)(A), because information even about their private lives may itself be foreign intelligence information because: For example, such information might identify their true status or reveal the intentions or activities of the foreign power of which they are officers or employees.

Paragraph (6) defines "electronic surveillance" to include three separate types of activities. Subparagraph (A) includes the acquisition, by an electronic, mechanical or other surveillance device, of the contents

of a wire communication without the consent of any party thereto when such acquisition occurs in the United States while the communication is being transmitted by wire. As this subdefinition makes clear, the location of the parties to the wire communication is immaterial if the acquisition occurs within the United States. Thus, either a wholly domestic telephone call or an international telephone call can be the subject of electronic surveillance under this subdefinition if the acquisition of the content of the call takes place in this country and if such acquisition occurs "while the communication is being transmitted by wire." This second qualifier is necessary because the definition of "wire communication" under 18 U.S.C. 2510(1) includes any communication "made in whole or in part" through wire facilities. Because most telephonic and telegraphic communications are transmitted at least in part by microwave radio transmissions, subdefinition (A) is meant to apply only to those surveillance practices which are effected by tapping into the wire over which the communication is being transmitted. The interception of the microwave radio transmission is meant to be covered by subdefinition (B) if the sender and all intended recipients are located within the United States.

Subparagraph (B) includes the acquisition by an electronic, mechanical, or other surveillance device of the contents of a radio communication, without the consent of any party thereto, made with a reasonable expectation of privacy where both the sender and all intended recipients are located within the United States, i.e., a totally domestic radio communication. This part of the definition would reach not only the acquisition of communications made wholly by radio but also the acquisition of "wire communications" by means of intercepting the radio transmitted portion of those communications where the communication is between persons who are all located within the United States. The territorial limits of this subdefinition are not dependent on the point of acquisition, as is the case with subdefinition (A), but on the locations of the communicants. Thus, the acquisition of radio communications outside the territorial limits of the United States would be covered if all of the communicants were located within the United States. Only acquisition of those domestic radio communications made with a reasonable expectation of privacy would be included in the term "electronic surveillance." This would exclude, for example, commercial broadcasts, as well as ham radio (47 U.S.C. section 605), and citizen band radio broadcasts. *United States* v. *Hall*, 488 F.2d 193 (9th Cir. 1973).

The effect of subparagraphs (A) and (B) of section 2521(b)(2), therefore, is to include within the term "electronic surveillance" the nonconsensual acquisition of all domestic radio communications made with a reasonable expectation of privacy, and the nonconsensual acquisition within the United States of all wire communications, as defined in 18 U.S.C. section 2510(1), except those international wire communications which are acquired by intercepting the radio transmitted portions of the communications.

The reason for excepting from the definition of "electronic surveillance" the acquisition of international radio transmissions, including international wire communications when acquired by intercepting radio transmissions, is to exempt from the procedures of the bill the signals intelligence activities of the National Security Agency.

Although it may be desirable to develop legislative controls in this area, the Committee has concluded that these practices are sufficiently different from traditional electronic surveillance techniques, both conceptually and technologically, that they should be considered separately by the Congress.[5] Attorney General Levi recognized this fact when he stated, in his testimony before a House subcommittee:

> Interception of international communications, beyond those covered by the bill, involves special problems and circumstances that do not fit the analysis and system this bill would impose. This is not to say that the development of legislative safeguards in the international communications area is impossible. I know it will be extremely difficult and will involve different considerations. I believe it will be unfortunate, therefore, to delay the creation of safeguards in the area with which this bill deals until the attempt is made to cover what is essentially a different area with different problems.[6]

The fact that this bill does not bring these activities within its purview, however, should not be viewed as congressional authorization of such activities. This committee merely recognizes, both in this definition and in section 2528(a), that this particular signals intelligence activity is not covered by the procedures outlined in this bill. In any case, the requirements of the fourth amendment would, of course, continue to apply to this type of communications intelligence activity.[7]

Subparagraph (C) brings within the definition of "electronic surveillance" the acquisition of information, not transmitted as a wire communication or radio communication, by the installation or use of an electronic, mechanical, or other surveillance device in the United States under circumstances in which a person has a constitutionally protected right of privacy. This is intended to include the acquisition of oral communications made by a person exhibiting an expectation that such utterances are not subject to acquisition, under circumstances justifying such expectation. In addition, it is meant to include the installation of beepers and "transponders," if a warrant would be constitutionally required in the ordinary criminal context. *United States* v. *Holmes*, 521 F. 2d 859 (5th Cir. 1975), *rehearing en banc granted*, 525 F. 2d 1364 (1976); *United States* v. *Martyniuk*, 395 F. Supp. 42 (D. Or. 1975). It could also include miniaturized television cameras and other sophisticated devices not aimed merely at communications.

This part of the definition is meant to be broadly inclusive, because the effect of including a particular means of surveillance is not to prohibit it but to subject it to judicial oversight. (See section 2528

---

[5] The nature of National Security Agency activities, the purposes of such activities and the technological problems associated with such activities have been carefully documented by the Church committee in vol. III, pages 733 et seq. See also, II Church committee 58–60, 108, and 308–311.

[6] Hearings before the *House Subcommittee on Courts, Civil Liberties and the Administration of Justice of the House Judiciary Committee, Foreign Intelligence Surveillance Act of 1976*, 94th Cong., 2d sess. 10–11 (1976) (hereinafter referred to as House Hearings).

[7] The committee notes with approval, however, that broadscale electronic surveillance of American citizens while abroad has been limited in part by both the President's Executive Order applicable to the foreign intelligence agencies and Department of Justice directives to the intelligence community. See *Executive Order* No. 11905, February 18, 1976; testimony of Attorney General Edward H. Levi before the *Church Committee*, November 6, 1975, p. 15. Thus, the surveillance of journalists such as Joseph Kraft would be prohibited.

infra.) It is not meant to include, however, the acquisition of those international radio transmissions or international wire communications, when acquired by intercepting radio transmissions, which are excluded from subparagraphs (A) and (B) of this paragraph. Nor, as earlier indicated, is it meant to require a court order in any case where a search warrant would not be required in an ordinary criminal context. It has been held, for example, that fourth amendment protections do not extend to activities undertaken in the open where a participant could reasonably anticipate that his activities might be observed. *Air Pollution Variance Board* v. *Western Alfalfa Corp.*, 416 U.S. 861 (1974). But two persons in a public park, far from any stranger, would not reasonably anticipate that their conversations could be overheard from afar through a directional microphone, and so would retain their right of privacy. Of course, law enforcement officers may, if they wish, continue to obtain an ordinary search warrant or chapter 119 court order if the facts and circumstances so justify it.

The definition of "electronic surveillance" comprising the interception of wire communications and radio transmissions has an explicit exception where any party has consented to the interception. This is intended to continue the law regarding consensual interceptions found in 18 U.S.C. section 2511(2)(c) and in the case law interpreting 47 U.S.C. section 605. *Lopez* v. *United States*, 373 U.S 427 (1963); *Rathbun* v *United States*, 355 U.S. 197 (1957). Whether consent may be inferred in a particular case will depend on the facts and circumstances.

That part of the definition of "electronic surveillance" comprising the installation of a device requires that the acquisition of information be under circumstances in which a person has a constitutionally protected right of privacy. There is no such right in those situations where the interception is consented to by at least one party to the conversation. For instance, a body microphone placed on an informer with his consent is an installation of a device to acquire information, but a person speaking to the informer has no justifiable expectation that the informer will not repeat, record, or even transmit by a miniature transmitter what the person voluntarily tells the informer. By telling the informer something, the person has, with respect to that information, surrendered his expectation of privacy vis-a-vis the informer. Such a situation is not, of course, limited to body microphones. Telephone conversations to which one of the parties has consented and microphones installed with consent would be functionally equivalent. What is important is the consent. So long as one party to the conversation has consented to the surveillance, the other party has no justifiable expectation of privacy in which he voluntarily reveals to the party who has consented to the surveillance. *United States* v. *White*, 401 U.S. 745 (1971). Thus, the absence of a reasonable expectation of privacy where one party consents to the surveillance is the equivalent of the explicit consent provision in 18 U.S.C. section 2511(2)(c).

Paragraph (7) defines "Attorney General" to mean the Attorney General of the United States or, in his absence, the Acting Attorney General. Notwithstanding any other provision of law, the power to

act under this legislation may not be delegated by the Attorney General. (*Giordano* v. *United States*, 416 U.S. 505 (1974.)

Paragraph (8) defines "minimization procedures" as procedures which will minimize the acquisition of any information which is not foreign intelligence information, will assure that no information which is not foreign intelligence information will be maintained, and to assure that all foreign intelligence which is obtained will be used only as provided in Section 2526 of the bill.

Section 2522

This section authorizes the submission of applications to a judge for a court order approving the use of electronic surveillance under this chapter. Applications may be submitted only if the President has, by prior written authorization, empowered the Attorney General to approve the submission. This section does not require the President to authorize each specific application; he may authorize the Attorney General generally to seek applications under this chapter or upon such terms and conditions as the President wishes so long as the terms and conditions are consistent with this chapter.

Section 2523

Subsection (a) provides for the public designation by the Chief Justice of seven United States district court judges, any one of whom may hear applications and grant orders under this chapter. Each judge shall have nationwide jurisdiction, but the Committee contemplates that there will be some geographic dispersion among them.

The subsection provides that none of the designated judges shall have jurisdiction to hear an application for electronic surveillance if that application has been previously denied by another of the designated district judges. This provision is intended to make clear that if the government desires to pursue an application after a denial, it must seek review in the special court of review established in subsection (b), it cannot apply to another district judge.

The subsection further provides that a designated district judge who denies an application for electronic surveillance shall provide a complete written statement of the reasons for the denial, and, if the government seeks review of the decision, forward that statement and other elements of the record to the special court of review. This will ensure that the special court of review is fully informed of the proceedings in the district court as it reviews the case.

Subsection (b) provides for the public designation by the Chief Justice of three judges from the federal courts of appeals or district courts who shall sit together as a special court of review having jurisdiction to review denials of applications made to the individual judges designated in subsection (a). If the special court of review determines that an application was properly denied, it shall provide a written statement of the reasons for its decision and, if the government seeks to appeal, forward the complete record to the Supreme Court, which will have jurisdiction to review the decision.

Subsection (c) provides for the expeditious handling of all proceedings under this chapter and also states that the Chief Justice, in consultation with the Attorney General, shall establish security measures under which applications made and orders granted shall be maintained. The Committee contemplates that the record of applications made and

orders granted by the several judges designated under this chapter shall be maintained in such a way that the judges designated under this chapter shall have access to the records of actions taken by the other judges similarly designated.

The Select Committee's amendments to Section 2523 as reported by the Judiciary Committee added provisions for the public designation of judges, the denial of jurisdiction of designated district judges to hear applications previously denied by another district judge, and the forwarding of a complete record of proceedings to the higher court in each stage of the review proceedings.

Section 2524

This section is patterned after 18 U.S.C. section 2518 (1) and (2), and specifies what information must be included in the application. Applications must be made in writing and under oath or affirmation by a federal officer. If the officer making the application is unable to verify personally the accuracy of the information or representations upon which the application is based, the application must also include affidavits by investigative or other officers who are able to provide such personal verification. Thus, for example, if the applicant was an attorney in the Department of Justice who had not personally gathered the information contained in the application, it would be necessary that the application also contain an affidavit by the investigating officer personally attesting to the status and reliability of any informants or other covert sources of information. By this means the source of all information contained in the application and its accuracy will have been sworn to by a named official of the United States Government and a chain of responsibility established for judicial review.

Each application must be personally approved by the Attorney General, who may grant such approval if he finds that the appropriate procedures have been followed. The Select Committee amended this section to make perfectly clear that the Attorney General's approval was discretionary rather than mandatory. The Attorney General shall also state in writing his belief that the facts and circumstances relied upon for the application would justify a judicial finding of probable cause that the target is an agent of a foreign power and that the facilities or place at which the electronic surveillance is directed are being used, or about to be used, by an agent of a foreign power, and that all other statutory criteria have been met. In addition, the Attorney General must personally be satisfied that the certification made pursuant to paragraph (8) of subsection (a) is proper in all respects.

Paragraph (1) of subsection (a) requires that the application identify the federal officer making the application; that is, the name of the attorney who actually presents the application to the judge.

Paragraph (2) requires that the application contain evidence of the authority of the applicant to make this application. This would consist of the presidential authorization to the Attorney General and the Attorney General's approval of the particular application.

Paragraph (3) requires the identity or characterization of the person who is the target of the electronic surveillance. The Select Committee changed this paragraph by inserting the word "target" for "subject" in order to more precisely define the information required. The word "person" is used in its juridical sense to mean the individual

or entity that is the target of the surveillance. However, care must be taken in framing the order authorizing such surveillance (and minimization procedures) that surveillance against one individual does not lead to the interception of communications of an entire group or organization, thus violating constitutional rights of association and privacy.

Paragraph (4) requires a statement of the facts and circumstances justifying the applicant's belief that the target of the electronic surveillance is a foreign power or an agent of a foreign power and that the facilities or place at which the surveillance is directed are being used or are about to be used by that power or agent. These requirements parallel existing law. (18 U.S.C. section 2518(1)(b)(ii) and (iv))

Paragraph (5) requires a statement of the procedures by which the acquisition, retention, and dissemination of information relating to the United States citizens and permanent resident aliens is to be minimized and expunged from the government's files. Such procedures should include limitations on retention and dissemination as well as provisions for the destruction of irrelevant information.

Because the Select Committee believes that it is essential that the invasion of the privacy of permanent resident aliens and American citizens caused by electronics surveillance be limited to the maximum extent possible, it amended this paragraph to require not only a statement of the procedures to minimize the acquisition and retention of information which is not foreign intelligence information, but also a statement of the procedures to minimize this "dissemination and to require the expunging" of such information.

The Committee also added a provision that appropriate steps be taken to prevent foreign intelligence information which relates solely to the conduct of foreign affairs from being maintained in a way that would permit retrieval by reference to a U.S. citizen who is a party to an intercepted communication. This requirement is intended to strike a balance between individual rights and government needs in the delicate situation where American citizens are overheard in conversations which contain information solely related to the conduct of foreign affairs.

There is no perfect solution to this problem. As long as the surveillance was instituted lawfully, the person's conversation may legally be overheard. Because the subject matter of the conversation is foreign intelligence information, it should not be excluded by minimization procedures.

However, the Committee believes that every effort should be made to minimize the "chilling effect" that retention of such conversations of Americans will have. The Committee amendment provides that when the Government files a conversation of this sort for retrieval and use at some future time, the conversation should be filed or indexed only according to the subject matter of the conversation. No file should be started or maintained under the name of the American citizen when the information relates solely to the conduct of foreign affairs.

The statement of procedures required under this paragraph should be full and complete and subject to the closest judicial scrutiny. These procedures may differ from case to case, depending on the nature of agency relationships, the individuals using the facilities or place to be

surveilled, the type of foreign intelligence information sought, and other similar factors. Minimization procedures should normally include such elements as methods to avoid the acquisition of irrelevant information at the time of intercept, restrictions on the use of surveillance to times when foreign intelligence information is likely to be obtained, provisions for terminating surveillance if it does not produce results of the specified type, and requirements for regular periodic review and deletion of information obtained which is not foreign intelligence information.

For example, steps should be taken to prevent untoward invasion of the privacy of a target's family by a twenty-four hour tap on his phone when it is known that the target is out of town or at the office. Similarly, conversations unrelated to foreign intelligence, such as those related to the personal life of the target or his family, should not be permitted to accumulate on tapes.

Paragraph (6) was added by the Select Committee to provide special protection for permanent resident aliens and citizens of the United States who are employed by an entity controlled and directed by a foreign government or governments, which is the target of electronic surveillance and which is not substantially composed of officers or employees of a foreign government, or individuals who are agents of a foreign power as defined in Section 2521(2)(B), (C), (D), or (E). In such cases, the government must, in addition to the statement of procedures required by paragraph (5), present a statement of procedures to prevent the acquisition, retention, and dissemination of, and to require the expunging of, communications of permanent resident aliens and citizens who are not officers or executives of the entity responsible for activities which involve foreign intelligence information. Again, the Committee contemplates a full and complete statement of procedures in order that the judge can properly examine the manner in which the surveillance will be conducted, and if the government fails to demonstrate that, for all practical purposes, there will be prevention of the acquisition of the communications specified, the application will be deficient.

The Committee recognizes that in some cases it may be impossible to prevent such acquisition completely, but this section requires that the Government must show it will prevent acquisition in an overwhelming majority of instances.

Paragraph (7) was also added by the Select Committee. It calls for a factual description of the nature of the information sought by the electronic surveillance. The description should be as specific as possible and sufficiently detailed that it clearly states what the government seeks. A simple designation as to which subdefinition of "foreign intelligence information" is involved will not be sufficient.

Paragraph (8) requires a certification or certifications by the Assistant to the President for National Security Affairs and/or by an appropriate executive official appointed by the President with the advice and consent of the Senate. The certification would be made by the official having ultimate responsibility for establishing requirements for the collection of the information—normally the Assistant to the President for National Security Affairs, the Director of the Central Intelligence Agency or the Director of the Federal Bureau of Investigation—and/or such other officer, appointed with the ad-

vice and consent of the Senate, who has full knowledge of the case. The Select Committee provided for the possibility of additional certifications to ensure that a detailed and complete certification is presented to the judge.

The certification shall state that the information sought is foreign intelligence information, that the purpose of the surveillance is to obtain foreign intelligence information, and that such information cannot feasibly be obtained by normal investigative techniques. It shall include a designation of what type of foreign intelligence information is sought and a reasoned articulation of the basis for certifying that the information sought is foreign intelligence information and cannot feasibly be obtained by other investigative techniques.

The purpose of the certification that the information sought is "foreign intelligence information" is to require that a high-level official certify and explain the determination that the information sought is in fact foreign intelligence information. The requirement that this judgment be explained was added by the Select Committee to ensure that those making certifications carefully consider the cases before them and avoid the temptation to simply sign off on certifications which consist largely of boilerplate language. The designated official must similarly explain in his affidavit why the information cannot be obtained through less intrusive techniques. This requirement is particularly important in those cases when United States citizens or resident aliens are the target of the surveillance.

The certification must also include a statement that the purpose of the surveillance is to obtain the described foreign intelligence information. This requirement is designed to prevent the possibility of targeting one individual for electronic surveillance when in fact another individual is the intended target of the attempt to gather information. It is also designed to make explicit that the sole purpose of such surveillance is to secure a foreign intelligence information and not to obtain information for any other purpose.

Paragraph (9) requires the application to contain a statement of the means by which the surveillance will be effected. It will generally be sufficient if the application indicates whether the information will be acquired by means of a wiretap, a microphone installation, the interception of a radio signal or some other means.

Paragraph (10) parallels 18 U.S.C. section 2518(1)(e) and requires a statement concerning all previous applications dealing with the same person, facilities, or places and disposition of each such previous application. The Committee deleted language which implied that there could be applications of which the Attorney General was unaware.

Paragraph (11) parallels 18 U.S.C. section 2518(1)(e) and requires a statement as to the period of time for which the surveillance is necessary. If the surveillance order is not to terminate automatically when the information sought has been obtained, the applicant must provide additional facts supporting his belief that additional information of the same type will be obtained thereafter.

Subsection (b) allows the Attorney General to require other executive officers to provide information to support the application.

Subsection (c) enables the judge to require the applicant to furnish further information as may be necessary to make the proper deter-

mination. It parallels existing law, 18 U.S.C. section 2518(2). Such additional proffers would, of course, be made part of the record.

Section 2525

Subsection (a) of this section is patterned after 18 U.S.C. section 2518(3) and specifies the findings the judge must make before he grants an order approving the use of electronic surveillance for foreign intelligence purposes. While the issuance of an order is mandatory if the judge finds that all of the requirements of this section are met, the judge has the discretionary power to modify the order sought, such as with regard to the period of authorization or the minimization procedures to be followed.

Paragraph (1) of this subsection requires the judge to find that the President has authorized the Attorney General to approve such applications.

Paragraph (2) requires the judge to find that the Attorney General has approved the application being submitted and that the application has been made by a federal officer.

Paragraph (3) requires a finding that there is "probable cause" to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power and that the facilities or place at which the surveillance is directed are being used or are about to be used by that power or agent.

In determining whether probably cause exists under this section, the court must consider the same requisite elements which govern such determinations in the traditional criminal context. Such elements include, for example, the issue of any informant's reliability, the circumstances under which the informant was able to learn about the alleged activity of the individual who is the subject of the warrant, the length of time which has passed since the information relied upon was acquired, and the degree to which information corroborating an informant must relate to the essential conduct on which the application is premised and not merely to incidental details.

In addition, in order to find "probable cause" to believe the subject of the surveillance is an "agent of a foreign power" under subsection 2521(b) (2) (B), (C), (D), or (E) the judge must, of course, find that the Government has established probable cause that each and every element of that status exists. For example, if an American citizen or resident alien is alleged to be engaged in terrorist activities for or on behalf of a foreign power, there must be probable cause to believe the person is knowingly acting for or on behalf of a foreign power.

Further there must be probable cause to believe that the efforts undertaken by the person on behalf of the foreign power constitute terrorism as defined in section 2521.

Similar findings of probable cause are required for each element necessary to establish that an American is conspiring with or aiding and abetting someone engaged in sabotage, terrorism, or clandestine intelligence activities for or on behalf of a foreign power. To continue the terrorism example, the findings would include a probable cause finding that the individual knows the person he is conspiring with or aiding or abetting is engaged in terrorist activities for or on behalf of a foreign power.

As indicated earlier, a judicial determination that a person is an agent of a foreign power as defined in Section 2521(b)(2)(E) requires careful findings by the Court. The judge must find that the person is part of a foreign intelligence network, that is, that he is acting pursuant to the direction of a foreign intelligence service network which engages in intelligence activities in this country for a foreign power. He must find that the person is knowingly transmitting information or material to that service or network in a covert manner and that the circumstances surrounding the activity taken together are so compelling that a reasonable man would have to conclude that the information or material transmitted to the nework will be used to harm the security of the United States, or that lack of knowledge of the transmission would harm our national security.

In order to determine whether the requisite probable cause has been established, the judge may request such additional information as he deems necessary in light of the facts and circumstances upon which the application for an order relies.

Paragraphs (4) and (5) require the judge to find that the procedures described in the application to minimize, and in the case of paragraph (5) to prevent, the acquisition, retention, and dissemination, and to require the expunging, of certain information or communications described previously relating to permanent resident aliens or American citizens are reasonably designed to accomplish their purpose. The Committee contemplates that the judge would give these procedures most careful consideration. If he does not believe they will be effective, the application should be denied. The Committee realizes that total expunging of bits and pieces of the original tape recording may be impossible. Moreover, it may not be possible to determine at once that certain information is irrelevant. Therefore, the bill's requirement is phrased in terms of the procedures being "reasonably designed" to require expunging. Thus, for example, it is expected that where irrelevant information cannot be erased from part of a tape, the procedures would prohibit dissemination of the tape and prohibit including such information in the logs or reports. In addition, where it cannot be immediately determined whether a certain piece of information is irrelevant, the procedures would require that within a specified reasonable time such a determination be made and the matter then expunged.

It should be noted that this provision contains one significant change from the provision in chapter 119. Section 2518 (8) (a) requires that all interceptions be recorded, if possible, and that the tapes not be edited or destroyed for ten years. In a criminal context the maintenance of such tapes and files under court seal insures that the interceptions will be retained in their original state so that if criminal prosecutions are undertaken it is clear that the evidence is intact and has not been tampered with. While there may be cases in which information acquired from a foreign intelligence surveillance may be evidence relating to a crime, these cases are expected to be relatively few in number, unlike title III interceptions which are instituted in order to obtain evidence of criminal activity. The Committee believes that in light of the relatively few cases in which information acquired under this chapter may be used as evidence in a criminal trial, the better practice is to allow the destruction of information that is

neither foreign intelligence information as defined in the bill or evidence of criminal activity. This course will more effectively safeguard the privacy of individuals, ensuring that irrelevant information will not be retained. The Committee believes that existing criminal statutes relating to obstruction of justice will deter any efforts to tamper with evidence of criminal activity acquired under this chapter. As has been the experience in title III interceptions for criminal purposes, it may be impossible to eliminate the acquisition of all irrelevant information in all cases. Therefore, it becomes important to destroy irrelevant information inadvertently acquired. Such destruction should occur, of course, pursuant to procedures approved by the court.

Paragraph (6) requires that the judges find that the application contains the description and certification or certifications specified in section 2524(a) (7) and (8). If the application meets the requirement of those sections, the court is not permitted to substitute its judgment for that of the executive branch officials(s).

The Committee recognizes that, by not allowing the court to determine whether or not the information sought is "foreign intelligence information" which cannot be obtained by other inevstigative techniques, an argument can be made that the court is doing little more than providing a rubber stamp for executive action. There are several points to be considered. First, the court, not the executive branch, makes the finding of whether or not probable cause exists that the target of the surveillance is a foreign power or its agent. It is this finding that constitutes a fundamental safeguard for the individual. It is also an effective external control on arbitrary executive action. Second, the certification procedure assures written accountability within the executive branch for the decision made to engage in such surveillance. This constitutes an internal check on executive branch arbitrariness.

Moreover, it should be noted that if the description and certification do not fully comply with sections 2524(a) (7) and (8), they can and must be rejected by the court. Thus, the court could invalidate the certification if it were not properly signed by the President's designee, did not designate the type of information sought, or did not state that the information sought is foreign intelligence information, that the purpose of the surveillance is to obtain foreign intelligence information, and that such information cannot feasibly be obtained by normal investigative techniques. Further, if the certification did not present an explanation of the judgment that the information sought is foreign intelligence information which cannot be obtained through normal investigative techniques, the judge could reject the application or defer approval until an adequate certification has been supplied.

Subsection (b) specifies what the order approving the electronic surveillance must contain. It must include the identity or a characterization of the person or persons targeted by the electronic surveillance. The order must specify the place or facilities against which the surveillance is directed. The order must also specify the type of information sought. These requirements are designed to satisfy the Fourth Amendment's requirements that warrants describe with particularity and specificity the person, place, and objects to be searched or seized. The order must, in addition to the Fourth Amendment's requirements,

specify the means by which the surveillance will be effected. Finally, the order must specify the period of time during which the surveillance is approved.

The order shall direct that the minimization procedures will be followed. It is intended that the court shall monitor compliance with the minimization procedures in much the same way as has been done pursuant to chapter 119. Failure to abide by the minimization procedures may be treated as contempt of court.

The order may also direct that a common carrier, landlord, custodian, contractor or other specified person furnish information, facilities or technical assistance necessary to accomplish the electronic surveillance successfully and with a minimum of interference to the services provided by such person to the target of the surveillance. If the judge directs such assistance, he shall also direct that the applicant compensate the person for such assistance. These provisions generally parallel 18 U.S.C. 2518(4).

This directive provision must be read in conjunction with the bill's conforming amendment to 18 U.S.C. 2511(2)(a)(ii), contained in section 4(b) of this bill. That amendment requires that before a communication common carrier or its agent provides such information, facilities or technical assistance to an investigative or law enforcement officer, that officer is required to furnish to the carrier either an order signed by the authorizing judge certifying that a court order directing such assistance has been issued or, in the case of surveillance undertaken under chapter 119 or 120 in which a prior order is not required, a sworn statement by the officer certifying that the applicable statutory requirements have been met.

Subsection (c) allows an order approving electronic surveillance under this chapter to be effective for the period necessary to achieve its purposes or for 90 days, whichever is less. In the Committee's view 90 days is the maximum length of time during which a surveillance for foreign intelligence purposes should continue without new judicial scrutiny. This period of time is not as long as some have wished but longer than others desired. It is considered to be a reasonable condition in the foreign intelligence context. (*United States* v. *United States District Court*, 407 U.S. 297 at 323 (1972)).

As under chapter 119, extensions of an order may be sought and granted on the same basis as the original order. A new application, including a new certification pursuant to section 2524(a)(5), would therefore be required. updating the information previously provided. Before the extension should be granted, however, the court would again have to find probable cause that the target is a foreign power or its agent. To aid the judge in making this determination anew, the Select Committee added language to make clear that he has the right to require the government to submit information obtained pursuant to previous orders for electronic surveillance or any other evidence that he deems necessary. It is expected that the success or failure of previous surveillance or the nature of the information obtained from such surveillance will often be important to his determination.

Subsection (d) authorizes the Attorney General to approve an emergency electronic surveillance prior to judicial authorization under certain limited circumstances. First. the Attorney General must determine that an emergency situation exists which requires the employ-

ment of electronic surveillance before an order authorizing such surveillance can with due diligence be obtained. In addition, the factual basis for the issuance of an order under this chapter must be present.

The procedures under which such an emergency surveillance is authorized are considerably stricter than those of the comparable provision in chapter 119, 18 U.S.C. section 2518(7). First, only the Attorney General may authorize such emergency surveillance, whereas in 18 U.S.C. section 2518(7) the Attorney General may designate "any investigative or law enforcement officer" to authorize emergency interceptions under that subsection. Second, the Attorney General or his designee must contemporaneously notify one of the designated judges that an emergency surveillance has been authorized. There is no comparable requirement in 18 U.S.C. section 2518(7). Third, an application for an order approving the surveillance must be made to that judge within 24 hours; 18 U.S.C. section 2518(7) requires the application to be made within 48 hours. Fourth, the emergency surveillance cannot continue beyond 24 hours without the issuance of an order; under 18 U.S.C. section 2518(7) the emergency surveillance may continue indefinitely until the judge denies the application. Fifth, the Attorney General must order that minimization procedures required by this chapter for the issuance of a judicial order be followed during the period of the emergency surveillance. There is no comparable provision under 18 U.S.C. 2518(7). The Committee added the last provision because of its concern that as much as possible be done to eliminate the acquisition, retention and dissemination of information which is not foreign intelligence information in all circumstances. Its intent is to place the Attorney General in the role of the judge in authorizing surveillance during the 24 hour emergency period. He must examine minimization procedures as the judge would normally do under paragraphs (a) (4) and (5) of this section and order that the appropriate procedures be followed just as if he were granting a judicial order.

The Committee wishes to emphasize that the application must be made for judicial approval even if the surveillance is terminated within the 24 hour period and regardless of whether the information sought is obtained. This requirement ensures that all emergency surveillances initiated pursuant to this chapter will receive judicial review and that judicial approval or denial will be forthcoming *nunc pro tunc*. Thus, the termination of an emergency surveillance before the expiration of the twenty-four hour period shall not be a basis for the court failing to enter an order approving or disapproving the subsequent application. It is necessary for both the Justice Department and congressional oversight committees to have available a complete record both of the bases for such emergency surveillance authorization and of the judicial determinations of their legality under the statutory standard.

This provision for emergency authorization of surveillance by the Attorney General may not be utilized pending an appeal under section 2523, following the denial of an application for a judicial order. Under such circumstances, the Attorney General could not reasonably determine that "the factual basis for the issuance of an order under this chapter to approve such surveillance exists," as required by this subsection.

If the application is subsequently denied, or if the surveillance is terminated without an order eventually being sought (which, as already indicated, would constitute an unlawful act under this subsection), no information obtained or evidence derived from the surveillance shall be received, used or disclosed by the Government in any trial hearing or other proceeding before any court, grand jury, department, office, agency, regulatory body, legislative committee or other Federal, state or local authority. This exclusionary provision is designed to be absolute.

Subsection (e) provides that any denial of an order under this section, whether it be a denial of an application for an order for electronic surveillance, a denial of an application for an extension, or a denial of an application for an order approving an emergency electronic surveillance, shall include a statement of the reasons for such denial. This is both to instruct the Attorney General and to facilitate review on appeal, if an appeal is sought. It is expected that such statement would be contemporaneous with the denial and would be in writing. The statement should be kept secure under the same procedures as applicable to applications and orders under section 2523(c).

Section 2526

This section sets forth the permissible uses which may be made of information acquired by means of electronic surveillance conducted pursuant to this chapter. The fact that effective minimization may be more difficult in the foreign intelligence area than in the more traditional criminal area, and that this chapter contains less restrictive procedures than does chapter 119 (for example, 90 days of surveillance per order rather than 30 days), mandates that the uses to be made of the information acquired by means of this chapter be carefully restricted. This section, therefore, places more stringent restrictions on use and dissemination than does the corresponding provision of title III, 18 U.S.C. 2517.

Subsection (a) requires that information acquired from electronic surveillance conducted pursuant to this chapter may be used by Federal officers and employees only for purposes relating to the ability of the United States to protect itself against actual or potential attack or other grave hostile acts of a foreign power or foreign agent, to provide for the national defense or security of the nation; to provide for the conduct of foreign affairs; to protect against the terrorist or sabotage activities of a foreign power or an agent of a foreign power; to protect itself against the clandestine intelligence activities of an intelligence service or network of a foreign power or an agent of a foreign power; or for the enforcement of the criminal law. Thus the lawful use of foreign intelligence information gathered pursuant to this chapter are carefully restricted to actual foreign intelligence purposes and the enforcement of the criminal law.

The Select Committee eliminated the provisions in this subsection which restricted disclosure of information acquired from an electronic surveillance to Federal officers and employees in order to permit disclosure outside of the Federal government under certain limited circumstances. First, the Committee believes that dissemination should be permitted to state and local law enforcement officials. If Federal agents monitoring a foreign intelligence surveillance authorized under

this chapter were to overhear information relating to a violation of state criminal law, such as homicide, the agents could hardly be expected to conceal such information from the appropriate local officials.

Second, the Committee can conceive of situations where disclosure should be made outside of all government channels. Federal agents may learn of a terrorist plot to kidnap a business executive, for example. Certainly in such cases, they should be permitted to disclose such information as is necessary to the executive and his company to provide for the executive's security.

Third, the Committee believes that information concerning crimes, espionage activities, or the acts and intentions of foreign powers acquired by electronic surveillance may in some circumstances be appropriately disseminated to cooperating intelligence services of other nations. Certain nations cooperate with us in this manner, and so long as all the procedures of this chapter are followed by the Federal officers, including minimization and the limitations on dissemination, this cooperative relationship should not be destroyed by a blanket prohibition on dissemination to foreign intelligence services of information acquired by electronic surveillance. The Committee wishes to stress, however, that any such dissemination be carefully reviewed to insure that information acquired under this chapter concerning United States citizens or permanent resident aliens given to foreign intelligence services is not only generally disclosable to other federal officers but that there exists compelling reasons why disclosure to foreign intelligence services is necessary.

Disclosure in such compelling circumstances as the kidnap case, to local officials for the purpose of enforcing the criminal law, and to foreign intelligence services under the circumstances described above are generally the only exceptions to the rule that dissemination should be limited to Federal officials.

The Committee is very sensitive to possible abuse which can arise through indiscriminate dissemination of information outside of Federal channels. The FBI's COINTELPRO (counter-intelligence program) under which political information regarding certain individuals was given to employers in order to induce the employers to discharge those individuals, provides a prime example. Such disclosure of information is strictly forbidden by this subsection and intolerable in a free society.

This subsection also notes that no otherwise privileged communication obtained in accordance with or in violation of this chapter shall lose its privileged character. This provision is identical to 18 U.S.C. 2517(4) and is designed, like its title III predecessor, to change existing law as to the scope and existence of privileged communications only to the extent that it provides that otherwise privileged communications do not lose their privileged character because they are intercepted by a person not a party to the conversation.

Subsection (b) must be read in conjunction with the minimization requirements of section 2524(a)(5) and (6) and 2525(a)(4) and (5) and with the preceding subsection (a). As previously noted, the minimization procedures mandated by the court are designed to restrict the acquisition of information obtained by means of electronic surveillance to the foreign intelligence information sought. However, even the most thorough minimization efforts may result in the acquisition

of some information which is not foreign intelligence information. This subsection states that such information which is evidence of a crime may be retained and disclosed for law enforcement purposes. Such disclosure would, of course, be restricted by the provisions of subsection (a).

Such information must be acquired lawfully, however. This requires that there be a good faith effort to minimize. *United States* v. *Armocida*, 515 F. 2d 29 (3rd Cir. 1975). Thus, for example, if monitoring agents choose to disregard the minimization standards and thereby acquire evidence of a crime against an overheard party whose conversations properly should have been minimized, that evidence would be acquired in violation of this chapter and would properly be suppressed if offered at any official proceeding.

The Select Committee added an additional requirement that the disclosure must be accompanied by a statement that such evidence, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General. This provision was designed to eliminate circumstances in which a local prosecutor had no knowledge that evidence was obtained through electronic surveillance. In granting approval of the use of the evidence, the Attorney General would alert the prosecutor to the surveillance, and he, in turn, would alert the court under subsection (c).

Subsection (c) sets forth the procedures under the bill whereby information acquired by means of electronic surveillance may be received in evidence or otherwise used or disclosed in any trial, hearing or other proceeding before a Federal or state court. Although the primary purpose of electronic surveillance conducted pursuant to this chapter will not be the gathering of criminal evidence, it is contemplated that such evidence may occasionally be acquired; this subsection and the succeeding one establish the procedural mechanisms by which such information may be used in judicial proceedings.

At the outset the committee recognizes that nothing in subsection (c) abrogates the rights afforded a criminal defendant under *Brady* v. *Maryland*, 373 U.S. 83 (1963) and the Jencks Act (18 U.S.C. 3500 et. seq.). These legal principles inhere in any such proceeding and are wholly consistent with the procedures detailed here. Furthermore, nothing contained in this section is intended to alter the traditional principle that the Government cannot use material at trial against a criminal defendant, and then withhold from him such material, if it would otherwise be available to him, on the grounds that such disclosure would threaten the national security. *United States* v. *Andolschek*, 142 F. 2d 503 (2nd Cir. 1964).

Subsection (c) states that no information acquired pursuant to this chapter may be used unless, prior to the trial, hearing, or other proceeding, or at a reasonable time prior to an effort to disclose the information or submit it in evidence, the government notifies the court that such information was acquired by means of electronic surveillance conducted pursuant to this chapter. Upon such notification, the Government must make available to the court a copy of the court order and accompanying application upon which the surveillance was based.

The court must then conduct an in camera inspection of these materials as well as any other documents which it deems necessary, to determine whether the surveillance was authorized and conducted in a

manner which did not violate any constitutional or statutory right of the person against whom the evidence is sought to be introduced. The subsection further provides that in making such a determination, the court shall order disclosed to the person against whom the evidence is to be introduced the court order or accompanying application, or portions thereof, if it finds that there is a reasonable question as to the legality of the surveillance and that disclosure would promote the determination of such legality or that disclosure would not harm the national security. Thus this subsection deals with the procedure to be followed by the trial court in determining the legality (or illegality) of the surveillance.

The question of how to determine legality of an electronic surveillance conducted for foreign intelligence purposes has never been decided by the Supreme Court. As Justice Stewart noted in his concurring opinion in *Giordano* v. *United States:*

> Moreover, we did not in *Alderman*, *Butenko* or *Ivanov*, and we do not today, specify the procedure that the District Courts are to follow in making this preliminary determination [of legality]. 394 U.S. 316 (1968)

The Committee views the procedures set forth in this subsection as striking a reasonable balance between an entirely in camera proceeding which might adversely affect the defendant's ability to defend himself, and mandatory disclosure in all cases, which might occasionally result in the wholesale revelation of sensitive foreign intelligence information.

In cases involving straightforward factual situations and readily distinguishable parties the court will likely be able to determine the legality of the surveillance without any disclosure to the defendant. In other cases, however, the question may be more complex because of, for example, indications of possible misrepresentation of fact, vague identification of the persons to be surveilled or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order. In such cases, the committee contemplates that the court will find a reasonable question as to the legality of the surveillance and order disclosure to the defendant to promote a resolution of that question. Even if disclosure is ordered, the statutory provision would allow the judge to excise any sensitive national security information from the documents before ordering them turned over to the defendant. There would always be disclosure in cases where the national security would not be harmed.

The committee notes that there may be cases where the court believes that disclosure is necessary because there is a reasonable question as to legality, but the government argues that to do so, even given the court's discretionary power to excise certain sensitive portions, would damage the national security. In such situations the Government must choose—either disclose the material or forego the use of the surveillance-based evidence. Indeed, if the Government objects to the disclosure, thus preventing a proper adjudication of legality, the prosecution would probably have to be dismissed.

The standards for disclosing information as set out above were established by the Select Committee. The provisions for disclosure

contained in the Judiciary Committee's bill called for discretionary disclosure only when disclosure would "substantially promote a more accurate determination of the legality of the surveillance and that such disclosure would not harm the national security." Thus, in cases where the national security was involved, there would be no disclosure no matter how complex the case. The Committee believes that this standard would deny the defendant the right to litigate the legality of surveillance in a great many cases and is inappropriate.

Subsection (d) parallels 18 U.S.C. 2518(10)(a) and provides a statutory vehicle by which a person who has been a subject of electronic surveillance and against whom evidence derived therefrom is to be or has been introduced or otherwise used or disclosed in any trial, hearing or proceeding may move to suppress the contents of any communication acquired by, or evidence derived from such electronic surveillance. The grounds for such a motion would be that (a) the communication was unlawfully intercepted, (b) the order of authorization or approval under which it was intercepted is insufficient on its face, or (c) the interception was not made in conformity with the order of authorization or approval.

The "subject" of electronic surveillance means an individual who was a party to the intercepted communication or was a person against whom the interception was directed. Thus the word is defined to coincide with the definition of "aggrieved person" in section 2510 of title III. See also *Alderman* v. *United States*, 394 U.S. 165.

One situation in which such a motion might be presented would be that in which the court orders disclosed to the party the court order and accompanying application under subsection (c) prior to ruling on the legality of the surveillance. Such motion would also be appropriate, however, even after the court's finding of legality if, in subsequent trial testimony, a Government witness provides evidence that the electronic surveillance may have been authorized or conducted in violation of the court order. This might be the case, for example, if the Attorney General's Executive Assistant were to testify that he, rather than the Attorney General, had reviewed and signed the Attorney General's name to the application authorization.

The most common circumstance in which such a motion might be appropriate would be a situation in which a defendant queries the government under 18 U.S.C. § 3504 and discovers that he has been intercepted by electronic surveillance even before the government has decided whether evidence derived from that surveillance will be used in the presentation of its case. In this instance, under the appropriate factual circumstances, the defendant might move to suppress such evidence under this subsection even without having seen any of the underlying documentation.

A motion under this subsection shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the movant was not aware of the grounds for the motion.

The subsection further provides that upon the filing of a motion, the judge may, in his discretion, make available to the defendant or his counsel for inspection such portions of the intercepted communications or evidence derived therefrom as the judge determines to be in the interests of justice. The judge is given broad discretion. He is empowered to disclose to the movant or his counsel copies of tapes,

transcripts, surveillance logs or other forms of evidence derived therefrom if disclosure is consistent with the interests of justice. This is to aid the defendant in determining whether any tainted evidence was derived from the illegal surveillance. The nature and extent of such disclosure would be dependent on the factual allegations contained in the defendant's motion. In the event that the motion is granted, the court must order that the contents of the communication acquired by electronic surveillance or evidence derived therefrom be suppressed.

Subsection (c) provides for notice to be served on United States citizens and permanent resident aliens who were targets of an emergency surveillance and, in the judge's discretion, on other citizens and resident aliens who were incidentally overheard, where a judge denies an application for an order approving an emergency electronic surveillance. Such notice shall be limited to the fact that an application was made, the period of the emergency surveillance, and the fact that during the period foreign intelligence information was or was not obtained.

This notice may be postponed for a period of up to ninety days upon a showing of good cause to the judge. Thereafter the judge may forego the requirement of notice upon a second showing of good cause.

The fact which triggers the notice requirement—the failure to obtain approval of an emergency surveillance—need not be based on a determination by the court that the target is not an agent of a foreign power engaged in clandestine intelligence activities, sabotage, or terrorist activities or a person aiding such agent. Failure to secure a warrant could be based on a number of other factors, such as an improper certification. A requirement of notice in all cases would have the potential of compromising the fact that the Government had focused an investigation on the target. Even where the target is not, in fact, an agent of a foreign power, giving notice to the person may result in compromising an on-going foreign intelligence investigation because of the logical inferences a foreign intelligence service might draw from the targeting of that individual. For these reasons, the Government is given the opportunity to present its case to the judge for initially postponing notice. After ninety days, during which time the Government may be able to gather more facts, the Government may seek the elimination of the notice requirement altogether. It is the intent of the Committee that if the Government can initially show that there is a reason to believe that notice might compromise an ongoing investigation, or confidential sources or methods, notice should be postponed. Thereafter, if the Government can show a likelihood that notice would compromise an ongoing investigation or confidential sources or methods, notice should not be given.

Section 2527

Subsection (a) requires the submission of annual reports to both the Congress and the Administrative Office of the United States Courts containing statistical information relating to electronic surveillance under this chapter. Specifically, the reports must include the number of applications made for orders and extensions; the number of orders or extensions granted, modified, and denied; the periods of time for surveillances which orders authorized; the actual duration of all surveillances; the total number of separate surveillances which were undertaken during the preceding calendar year (extensions of an order

would not be considered separate surveillances); and the number of surveillances terminated during the preceding calendar year. The statistics in these reports should present a quantitative indication of the extent to which surveillances under this chapter are used. These statistics will also provide a basis for further inquiry by appropriate oversight committees of the Congress.

Such congressional oversight is particularly important in monitoring the operation of this statute. By its very nature foreign intelligence surveillance must be conducted in secret. This bill reflects the need for such secrecy; judicial review is limited to a select panel and routine notice to the target is avoided. In addition, unlike the statutory scheme in Title III, it is not contemplated that most electronic surveillances conducted pursuant to this chapter will result in criminal prosecution. Indeed, it is expected that very few will result in criminal prosecutions.

Subsection (b) was added to the Judiciary Committee's bill to further emphasize the need for congressional oversight in the implementation and execution of the provisions of this bill. Specifically, it provides that nothing in chapter 120 shall limit the authority of the Select Committee to obtain information it may need to carry out its duties pursuant to Senate Resolution 400, 94th Congress, 2nd Session.

Senate Resolution 400 established the Select Committee and charged it with duties—

> to oversee and make continuing studies of the intelligence activities and programs of the United States government, and to submit to the Senate appropriate proposals for legislation and report to the Senate concerning such intelligence activities and programs.

Oversight of foreign intelligence surveillance goes to the very heart of the Select Committee's charge, and subsection (b) will give its duties statutory recognition.

In order to properly discharge its responsibilities, the Committee will need access to full and complete information regarding all electronic surveillances conducted for the collection of foreign intelligence information. Section 11 of Senate Resolution 400 requires the head of each department and agency to keep the Select Committee fully and currently informed with respect to intelligence activities, to furnish any information or document needed by the Committee regarding such activities, and to notify it upon discovery of any and all intelligence activities which constitute violations of the constitutional rights of any person, violations of law, or violations of Executive orders, Presidential directives, or departmental or agency rules or regulations. The Committee already is requiring the Executive branch officials to meet these requirements regarding electronic surveillance and other intelligence activities and intends to continue vigorous oversight in the future. In this regard the Committee, pursuant to Senate Resolution 400, has recently completed a review of the present electronic surveillance cases and will conduct similar reviews in the future.

Moreover, Section 5, in conjunction with this section, in requiring annual reports by the Committee on the implementation of this legislation, ensures that the Committee will have access to all materials necessary to conduct such studies and issue such reports.

Section 2528

This section must be read in conjuction with the conforming amendment contained in paragraph (d) of Section 4 which repeals section 2511(3) of Title 18, United States Code, the so-called "National Security Disclaimer" of Title III of the 1968 Omnibus Crime Control and Safe Streets Act. The effect of that repeal is to establish this section as the exclusive congressional statement on the question of the President's power to order electronic surveillance in circumstances and for purposes not covered by the statutes of the United States.

The section begins by stating that "Nothing contained in Chapter 119, section 605 of the Communications Act of 1934, or this chapter shall be deemed to affect the exercise of any constitutional power the President may have, subject to determination by the courts, to acquire foreign intelligence information by means of an electronic, mechanical or other surveillance device if. . . ." The purpose of this prefactory phrase is threefold.

First, it sets forth the sections of the United States Code which regulate the procedures by which electronic surveillance may be conducted within the United States and the statutory controls for the use and dissemination of information so acquired. If enacted, this chapter will constitute the sole and exclusive statutory authority under which electronic surveillance of a foreign power or its agent to obtain foreign intelligence information may be conducted within the United States. It will complement Chapter 119, which deals with electronic surveillance for law enforcement purposes and section 605 of the Communications Act of 1934, as amended, which restricts the dissemination of certain information transmitted by wire or radio.

Secondly, this section states that these statutory provisions shall not be deemed to affect the exercise of any constitutional power the President may ultimately be deemed to possess to engage in certain types of electronic surveillance under specified conditions enunciated in subparagraphs (a) and (b) of this section. The precise phrasing used—"any constitutional power the President may have, subject to determination by the courts," is designed to make it absolutely clear that this section constitutes neither a grant of, nor limitation on, such power nor a congressional recognition of such power. The phrase "subject to determination by the courts" was added by the Select Committee to underscore this point. This introductory paragraph is couched in neutral language; it simply states that if such presidential power exists nothing in the statute (or other statutes) shall affect its exercise in the circumstances enunciated in subsections (a) and (b).

The committee recognizes the legal debate being engaged in today over the question of whether or not a constitutional presidential power exists to undertake warrantless electronic surveillance against foreign powers or foreign agents engaged in foreign intelligence activities. The Church committee concluded that no such power exists (Vol. II, p. 325).[1] The Supreme Court, however, has not definitely passed on the issue, while the lower Federal courts remain split, some recognizing a power, *United States* v. *Brown*, 484 F. 2d 418 (5th Cir. 1973) cert. denied 415, U.S. 960 (1974) *United States* v. *Butenko*, 494 F. 2d 593 (3d Cir. 1974); while others have indicated that no such power exists,

[1] That committee concluded that "while the constitutional issue has not been resolved, the committee does not believe that the President has inherent power to authorize the targeting of an American for electronic surveillance without a warrant . . ."

Zweibon v. *Mitchell*, 516 F. 2d 584 (D.C. Cir. 1975) cert. denied —— U.S. —— (No. 75–1056, April 20, 1976).

Under our constitutional system, however, neither the Congress nor the Executive can be the final arbiter of this question. Only the Supreme Court can ultimately decide whether such power exists. Accordingly, the committee emphasizes the neutrality of the prefatory language.

Regardless of how this question is ultimately resolved, however, it is clear that the Supreme Court has recognized that Congress may legislate in areas, where, absent such legislation, a constitutional power of the executive may be found to exist. *Youngstown Sheet and Tube* v. *Sawyer*, 343 U.S. 579 (1952). In that landmark case, the Supreme Court rejected President Truman's argument that he had inherent constitutional authority to seize the steel mills to prevent strikes and insure continued steel production needed for the war effort. The decision was influenced in large measure by the fact that Congress, by passing the Taft-Hartley Act, had explicitly rejected seizure of the steel mills and enacted a legislative alternative to curb labor unrest. In his concurring opinion Justice Jackson wrote:

> When a President takes measures incompatible with the express or implied will of Congress, his power is at the lowest ebb, for then he can rely only upon his own constitutional power minus any Constitutional power of Congress over the matter. Courts can sustain exclusive presidential control in such a case only by disabling the Congress from acting upon the subject. (343 U.S. at 637).

The Attorney General, in testifying in support of this bill, recognized that the Congress may act to prescribe the conditions and procedures under which the President may exercise such power:

> The express provision that the bill is not to have effect beyond its scope would perhaps not be so critical if the section did not make clear the intent—an intent that I find clear from the bill as a whole—that within its scope and its intended coverage the bill's requirements are mandatory. . . . As you know, a difference of opinion may exist as to whether it is within the constitutional power of Congress to prescribe, by statute, the standards and procedures by which the President is to engage in foreign intelligence surveillances essential to the national security. I believe that the standards and procedures mandated by the bill are constitutional. The Supreme Court's decision in the *Steel Seizure* case seems to me to indicate that when a statute prescribes a method of domestic action adequate to the President's duty to protect the national security, the President is legally obliged to follow it. My view, of course, does not foreclose future administrations from arguing or acting upon the contrary position. Nor can Congress decide the constitutional question. But Congress can do what this bill clearly does: if it is constitutional to mandate the bill's requirements within its defined scope, it is the statute's intent to do so.[2]

[2] House Hearings, 10–11. See also Justice White's concurring opinion in the *Keith* case, supra at 338 n. 1, where he stated that "the United States did not claim that Congress is powerless to require warrants for surveillances that the President otherwise would not be barred by the Fourth Amendment from undertaking without a warrant."

Thus, by enacting this chapter, Congress is, to use Justice Jackson's phrase, "acting upon the subject," in this case, foreign intelligence electronic surveillance within the United States, thereby limiting any presidential power which may have existed in the absence of such enactment within the confines of the bill's defined scope.

The third purpose of the introductory clause to this section is to make absolutely clear that if such power does, in fact, exist, this statute recognizes that its exercise for the purpose of acquiring foreign intelligence information shall be limited to acquisitions "by means of an electronic, mechanical, or other surveillance device." Other investigative or intelligence gathering practices are not within the scope of this chapter.

Section 2528 continues by setting forth the only two classes of electronic surveillance for foreign intelligence purposes which are beyond the scope of legislation and as to which the warrant procedures of this chapter would, therefore, be inapplicable. Phrased differently, if the Executive is found to possess inherent power to engage in warrantless electronic surveillance, subparagraphs (a) and (b) list the only facts and circumstances under which such power could be exercised. In enacting this section, therefore, the Congress has made an effort to limit the scope of any power to the two categories listed in the section.

Subsection (a) exempts from the chapter foreign intelligence gathering by means of an electronic, mechanical or other surveillance device if the acquisition does not come within the definition of "electronic surveillance" contained in section 2521(b)(6). Specifically, this provision is designed to make clear that the legislation does not deal with the communications intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States. As to methods of acquisition which come "within the definition of electronic surveillance" in this bill, the Congress has declared that this statute, not any claimed presidential power, controls.

As already indicated, the activities of the National Security Agency pose particular conceptual and technical problems which are not dealt with in this legislation. Although many on the committe are of the opinion that it is desirable to enact legislation safeguards for such activity, the committe adopts the view expressed by the Attorney General during the hearings that enacting statutory controls to regulate the National Security Agency and the surveillance of Americans abroad raises problems best left to separate legislation dealing with charters and guidelines for the intelligence community.[3]

Subsection (b) delineates the second type of surveillance exempted from the bill's warrant procedures. This would be electronic surveillance for foreign intelligence purposes in which the facts and circumstances giving rise to the acquisition are so unprecedented and so potentially harmful to the United States that they cannot be reasonably said to have been within the contemplation of Congress in enacting this chapter or chapter 119.

It must be emphasized that this subsection is not an alternative to the 24-hour emergency provision of section 2525(d). Therefore, the

[3] For a discussion of NSA activities and proposed legislative controls, see II Church committee 58–60, 108 and 308–311. The problems posed by electronic surveillance of Americans overseas can be found at pages 305 and 306; see, also III Church committee 733, et seq.

mere existence of an emergency situation which precludes time to secure a prior judicial warrant is an insufficient basis for the President to invoke his inherent power and proceed outside of the requirements imposed by this chapter.

On the contrary, many situations which pose great danger to the nation can be envisioned in which this bill is intended to provide the exclusive applicable procedures for electronic surveillance in this country. For example, the Government might be seeking foreign intelligence information about an allegedly imminent threat of assassination or the theft of a nuclear weapon and its threatened employment for terrorist purposes. In such situations, the Attorney General could authorize emergency warrantless electronic surveillance procedures specified in section 2525(d).

Such situations are not envisioned by the committee as the type of "unprecedented" circumstances beyond the contemplation of Congress within the meaning of this section.

It should be noted that the facts and circumstances must not only be unprecedented, they must also be "so potentially harmful that they cannot be reasonably said to have been within the contemplation of Congress in enacting this chapter or chapter 119." The Committee believes that this standard could only be met by a factual situation of extreme impending peril.

It is not the intent of subsection (b), however, to permit an ongoing program of surveillance for a sustained period of time. Should some such an unprecedented threat arise, posing such danger to the nation as to warrant an assertion of power under this section, the language requires that the President transmit to the Select Committee and the Judiciary Committees of Congress, under a written injunction of secrecy if necessary, a statement setting forth the nature of such facts and circumstances within seventy-two hours of the initiation of the surveillance. The seventy-two hour reporting requirement was added by the Select Committee to the Judiciary Committee bill to ensure that the report required of the President is promptly transmitted if power is ever asserted under subsection (b).

The final sentence of this section recognizes that if the Supreme Court ultimately decides that the fourth amendment warrant requirement does not apply to foreign intelligence electronic surveillance which is beyond the scope of this chapter, the reasonableness standard of that amendment would still be operative and would provide the test by which the conduct of the surveillance would be subsequently judged. Finally, it provides that foreign intelligence information acquired by authority of the President based on the assertion of any such constitutional power may not be used or disclosed except as is necessary to implement that assertion of power.

Section 3

Section 2 delays the effective date of the act until 60 days following the designation of the first judge pursuant to section 2523 of this chapter. The purpose of this delay is to allow time for the development of the applications required under this bill and of security measures governing the submission of these applications to the courts. The 60 day delay will also prevent the situation where one judge will be forced to handle all of the applications.

CONFORMING AMENDMENTS

Section 4 serves the important purpose of integrating the new chapter 120 with the current electronic surveillance law found in chapter 119 of title 18, United States Code. Various provisions of chapter 119 are applicable to the electronic surveillance engaged in under the new bill and the conforming amendments in this section of S. 3197 are designed to make changes reflecting this fact. In addition, where certain provisions of chapter 119 should not encompass the surveillance procedures in S. 3197, conforming amendments so limit such sections:

(a) (1) and (2). These amendments are designed to establish the same criminal penalties for violations of this chapter as apply to violations of chapter 119. As amended, these sections will make it a criminal offense to engage in electronic surveillance "except as otherwise specifically provided in chapters 119 or 120—or otherwise authorized by a search warrant or order of a court of competent jurisdiction." Activities "otherwise authorized" would include certain forms of investigative techniques used for enforcement of the criminal law which are not regulated by chapter 119 but do fall under the definition of "electronic surveillance" of chapter 120. In such criminal cases, it would not be necessary for the government to follow the procedures of chapter 120. In all cases involving electronic surveillance for the purpose of obtaining foreign intelligence information, however, the prohibitions of 18 U.S.C. 2511 would apply.

(a) (3), (4), (5), and (6). These amendments make clear that chapter 119's prohibitions of disclosure and use of information, obtained through the interception of wire or oral communications in sections 2511(1) (c) and (d) also apply to disclosure and use of information obtained through electronic surveillance as defined in chapter 120.

The Committee found it necessary to review the Judiciary Committee's section 4(a) to make it perfectly clear that all governmental activities defined as electronic surveillance in S. 3197 were governed by the prohibition of section 2511.

The statute calls for a fine of not more than $10,000 or imprisonment for not more than five years, or both, for each violation.

(b)(1) This amendment adds radio communication to wire communication and extends the meaning of intercept to include "or otherwise acquire" to section 2511(2)(a)(i) which permits communication common carriers to engage in certain activities.

(b)(2) This amendment, when read in conjunction with section 2525(b)(2) (ii) and (iii), makes explicit the fact that a court order obtained under chapter 120 may direct an officer, employee or agent of a communications common carrier to provide certain assistance to the governmental agents implementing the order. The nature and scope of such assistance is intended to be identical to that which may be directed under section 2518(4)(e) of chapter 119. The amendment further provides that before the carrier may provide such information or assistance, whether under chapter 119 or 120, the governmental agent must furnish the carrier with an order signed by the court (but not necessarily the same order as authorizes the actual surveillance) if an order has been acquired, or a sworn statement by the agent that

all statutory requirements have been met if the surveillance is being conducted pursuant to the provisions of section 2518(7) of chapter 119 or sections 2525(d) or 2528 of chapter 120. The document so furnished must also set forth the period of time for which the surveillance is authorized and a description of the facilities from which the communication is to be intercepted. Any violation of this subsection by a carrier or its representative will render the carrier liable for the civil damages provided for in section 2520, subject, of course, to the good faith reliance defense contained therein.

(c)(1) This amendment makes explicit that an employee of the Federal Communications Commission may engage in electronic surveillance as well as intercept a wire or oral communication in discharge of monitoring responsibilities exercised by the Commission.

(c)(2) This amendment makes clear that it is legal to engage in electronic surveillance, as well as intercepting a wire or oral communication, if a party consents.

(c)(3) This amendment provides statutory authorization for the government to conduct tests of equipment which may result in the interception of certain domestic communications, as defined in section 2521(2)(ii). The testing of no other type of electronic surveillance equipment is authorized by this section.

All tests conducted pursuant to this provision must be in the normal course of official business by the governmental agent conducting the test and must be designed solely for determining the capability of equipment used for foreign intelligence gathering purposes or the existence or capability of equipment used by a foreign power or its agents.

In addition, the test period shall be limited to that necessary to determine such capability and shall in no instance exceed ninety days without the express approval of the Attorney General. The contents of any communication acquired as a result of the test or search shall be disclosed only to those officials conducting the test and shall be used and retained by them only for the purpose of the test. At the completion of the testing or search period, the contents so acquired shall be destroyed. The Committee contemplates that in all cases such testing will be approved by a senior official prior to the commencement of the testing period.

(d) This amendment repeals section 2511(3) of chapter 119 since this subsection is incompatible with the passage of chapter 120, section 2528.

(e) This amendment brings any electronic surveillance as defined in chapter 120 under the same statutory exclusionary rule as applies to chapter 119. This section imposes an evidentiary sanction for failure to comply with the provision of the chapter. It makes explicit that not only is the communication excluded but also any information obtained from electronic surveillance.

(f) This amendment makes explicit that the requirements for an application enumerated in subsection 2518(1) apply only to surveillance conducted pursuant to chapter 119, since chapter 120 contains its own requirements.

(g) This amendment makes explicit that the necessary elements of an order set forth in subsection 2518(4) apply only to surveillance

conducted pursuant to chapter 119, since chapter 120 contained its own requirements.

(h) This amendment makes explicit that the procedures for disclosure of the application and accompanying application under this subsection apply only to surveillances conducted pursuant to chapter 119 since chapter 120 contains its own requirements.

(i) This amendment makes explicit that the provision for a statutory suppression motion contained in this subsection applies only to surveillances conducted pursuant to chapter 119 since chapter 120 contains its own requirements.

(k) These amendments are designed to authorize the recovery of civil damages for violations of chapter 120 in the same manner and amounts as already provided for violations of chapter 119. The only category of individuals who would be exempted from the provisions of this section are agents of a foreign power as defined in section 2521 (b) (2) (A) of chapter 120.

Section 5 instructs the Senate Select Committee on Intelligence to make yearly reports beginning March 1, 1978, to the Senate concerning the implementation of this chapter, including but not limited to analysis and recommendations on amending, repealing, or allowing this chapter to continue in effect without amendment. This section was agreed upon in lieu of limiting the bill to a two-year period.

Due to the fact that the Select Committee on Intelligence is a new one beginning work in a new field, it has recognized the need to continually review the adequacy of such legislation. It is the hope of the Committee that this section will be the means to constantly upgrade and refine the law in this area.

Section 6 outlines the expedited procedures to be followed in enacting legislation embodying recommendations reported pursuant to section 5. This section was added to ensure that any legislative recommendations of this Committee with regard to unforeseen problems in the implementation of the bill be given priority on the floor of the Senate.

Section 6(a) gives the Select Committee on Intelligence thirty days to report out legislation following its own reporting that this chapter should be amended or repealed.

Section 6(b) states that after reporting out such legislation it will become the pending business of the Senate with time for debate equally divided between proponents and opponents and shall be voted on within three days.

Section 6(c) states that after passage such legislation is referred to the appropriate committee of the House and is to be reported out with its recommendation within thirty days. It then becomes the business of the House to be voted on within three days.

Section 6(d) states that if there is any disagreement in the legislation passed by both Houses conferees shall be appointed to make and file a report within seven days after the legislation is referred to the committee of conference. Regardless of any rules regarding printing delays the report is to be acted on by both Houses within seven days of the filing of the Conference report. If the conferees are unable to agree within three days they are to report back to their respective Houses in disagreement.

The Committee believes that the area of foreign intelligence electronic surveillance is extremely important involving the most precious rights of Americans and that these expedited procedures are necessary to insure that issues involving electronic surveillance are treated as promptly as possible.

Changes in Existing Law

In compliance with subsection (4) of rule XXIX of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic and existing law in which no change is proposed is shown in roman):

Omnibus Crime and Safe Streets Act, as Amended

Title III, Chapter 119—Wire Interception and Interception of Oral Communications

Section 2511. Interception and disclosure of wire or oral communications prohibited

(1) Except as otherwise specifically provided in this chapter *or chapter 120 or as otherwise authorized by a search warrant or order of a court of competent jurisdiction*, any person who—

(a) willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire or oral communication, *or under color of law, willfully engages in any other form of electronic surveillance as defined in chapter 120;*

* * * * * * *

(c) willfully discloses, or endeavors to disclose, to any other person the contents of any wire or oral communication *or information obtained under color of law by any other form of electronic surveillance as defined in chapter 120*, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication *or any other form of electronic surveillance as defined in chapter 120*, in violation of this subsection; or

(d) willfully uses, or endeavors to use, the contents of any wire or oral communication *or information obtained under color of law by any other form of electronic surveillance as defined in chapter 120*, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication *or any other form of electronic surveillance as defined in chapter 120*, in violation of this subsection; shall be fined not more than $10,000 or imprisoned not more than five years, or both.

(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 *or radio communication*, to intercept *or otherwise acquire*, 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 or property of the carrier of such communication;

* * * * * * *

(2)(a)(ii) It shall not be unlawful under this chapter for an officer, employee, or agent of any communication common carrier to provide information, facilities, or technical assistance to an investigative or law enforcement officer who, pursuant to this chapter *or chapter 120*, is authorized to intercept a wire or oral communication *or engage in electronic surveillance, as defined in chapter 120. Provided, however, That before the information, facilities, or technical assistance may be provided, the investigative or law enforcement officer shall furnish to the officer, employee, or agency of the carrier either:*

(1) An order signed by the authorizing judge certifying that a court order directing such assistance has been issued, or

(2) In the case of an emergency surveillance as provided for in section 2518 (7) of this chapter or section 2525(d) of chapter 120, or a surveillance conducted under the provisions of section 2528 of chapter 120, a sworn statement by the investigative or law enforcement officer certifying that the applicable statutory requirements have been met,

and setting forth the period of time for which the surveillance is authorized and describing the facilities from which the communication is to be intercepted. Any violation of this subsection by a communication common carrier or an officer, employee, or agency thereof, shall render the carrier liable for the civil damages provided for in section 2520.

(2)(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire communication, or oral communication, transmitted by radio *or otherwise engage in electronic surveillance as defined in chapter 120*, or to disclose or use the information thereby obtained.

(2)(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire or oral communication *or engage in electronic surveillance as defined in chapter 120*, where such person is a party to the communication, or one of the parties to the communication has given prior consent to such interception *or such surveillance.*

* * * * * * *

(2)(e) It shall not be unlawful under this chapter or chapter 120, or section 605 of the Communications Act of 1934 for an officer, employee, or agent of the United States in the normal course of his official duty, to conduct electronic surveillance as defined in section 2521 (b)(2) of chapter 120, for the sole purpose of determining the capability of equipment used to obtain foreign intelligence or the existence or capability of equipment used by a foreign power or its agents: Provided, (1) that the test period shall be limited in extent and duration to that necessary to determine the capability of the equipment; and (2) that the content of any communication acquired under this sec-

tion shall be retained and used only for the purpose of determining the existence or capability of such equipment, shall be disclosed only to the officers conducting the test, and shall be destroyed upon completion of the testing period; and (3) that the test may exceed ninety days only with the prior approval of the Attorney General.

[(3) Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143, 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation 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. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary 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. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial, hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.]

* * * * * * *

Section 2515. Prohibition of use as evidence of intercepted wire or oral communications

Whenever any wire or oral communication has been intercepted, *or electronic surveillance as defined in chapter 120 has been made*, no part of the contents of such communication *or other information obtained from electronic surveillance as defined in chapter 120*, and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

* * * * * * *

Section 2528. Procedure for interception of wire or oral communications

(1) Each application for an order authorizing or approving the interception of a wire or oral communication *under this chapter* shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application.

* * * * * * *

(4) Each order authorizing or approving the interception of any wire or oral communication *under this chapter* shall specify—

* * * * * * *

An order authorizing the interception of a wire or oral communication *under this chapter* shall, upon request of the applicant, direct that a communication common carrier, landlord, custodian or other

person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such carrier, landlord, custodian, or person is according the person whose communications are to be intercepted. Any communication common carrier, landlord, custodian, or other person furnishing such facilities or technical assistance shall be compensated therefore by the applicant at the prevailing rates.

* * * * * * *

(9) The contents of any [[intercepted]] wire or oral communication *intercepted pursuant to this chapter*, or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10) (a) 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 *intercepted pursuant to this chapter*, or evidence derived therefrom, on the grounds that—

* * * * * * *

SECTION 2519. Reports concerning intercepted wire or oral communications—

* * * * * * *

(3) In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire or oral communication *pursuant to this chapter* and the number of orders and extensions granted or denied *pursuant to this chapter* during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

Section 2520. Recovery of civil damages authorized

[[Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall (1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications, and]] *Any person other than an agent of a foreign power as defined in section 2521(b)(2)(A) of chapter 120, who has been subject to electronic surveillance as defined in chapter 120, or whose wire or oral communication has been intercepted, or about whom informa-*

tion has been disclosed or used, in violation of this chapter, shall (1) have a civil cause of action against any person who so acted in violation of this chapter and (2) be entitled to recover from any such person—

* * * * * * *

Chapter 120.—ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

Sec.

§ 2521. Definitions

(a) Except as otherwise provided in this section the definitions of section 2510 of this title shall apply to this chapter.

(b) As used in this chapter—

(1) "Foreign power" means—

(A) a foreign government or any component thereof, whether or not recognized by the United States;

(B) a faction of a foreign nation or nations, not substantially composed of permanent resident aliens or citizens of the United States;

(C) an entity, which is directed and controlled by a foreign government or governmens;

(D) a foreign-based terrorist group; or

(E) a foreign-based political organization not substantially composed of permanent resident aliens or citizens of the United States.

(2) "Agent of a foregn power" means—

(A) a person who is not a permanent resident alien or citizen of the United States and who is an officer or employee of a foreign power;

(B) a person who—

(i) knowingly engages in, or knowingly acts in furtherance of, terrorist activities for or on behalf of a foreign power, or

(ii) conspires with, aids, or abets such a person, knowing that such person is engaged in such activities;

(C) a person who—

(i) knowingly engages in, or knowingly acts in furtherance of, sabotage activities for or on behalf of a foreign power, or

(ii) conspires with, aids, or abets such a person, knowing that such person is engaged in such activities;

(D) a person who—

(i) knowingly engages in clandestine intelligence activities for or on behalf of a foreign power, which

activities involve or will involve a violation of the criminal statutes of the United States; or

(ii) conspires with, aids, or abets such a person, knowing that such person is engaged in such clandestine intelligence activities; or

(E) a person who, acting pursuant to the direction of an intelligence service or intelligence network which engages in intelligence activities in the United States on behalf of a foreign power knowingly transmits information or material to such service or network in a manner intended to conceal the nature of such information or material or the fact of such transmission under circumstances which would lead a reasonable man to believe that the information or material will be used to harm the security of the United States, or that lack of knowledge by the Government of the United States of such transmission will harm the security of the United States.

(3) "Terrorist activities" means activities which—

(A) are violent acts or acts dangerous to human life which are criminal under the laws of the United States or of any State if committed within its jurisdiction; and

(B) appear to be intended—

(i) to intimidate or coerce the civilian population, or

(ii) to influence the policy of a government by initimidation or coercion.

(4) "Sabotage activities" means activities prohibited by title 18, United States Code, Chapter 105.

(5) "Foreign intelligence information" means—

(A) information which relates to, and is deemed necessary to the ability of the United States to protect itself against, actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) information with respect to a foreign power or foreign territory, which relates to, and because of its importance is deemed essential to—

(i) the national defense or the security of the Nation, or

(ii) the conduct of the foreign affairs of the United States;

(C) information which relates to, and is deemed necessary to the ability of the United States to protect against, the terrorist activities of a foreign power; or an agent of a foreign power.

(D) information which relates to, and is deemed necessary to the ability of the United States to protect against, the sabotage activities of a foreign power; or an agent of a foreign power.

(E) information which relates to, and is deemed necessary to the ability of the United States to protect itself against, the clandestine intelligence activities of an intelligence service or network of a foreign power or an agent of a foreign power.

(6) "Electronic surveillance" means—

(A) the acquisition, by an electronic, mechanical, or other surveillance device, of the contents of a wire communication to or from a person in the United States, without the consent of any party thereto, where such acquisition occurs in the United States while the communication is being transmitted by wire;

(B) the acquisition, by an electronic, mechanical, or other surveillance device of the contents of a radio communication, without the consent of any party thereto, made, under circumstances where a person has a constitutionally protected right of privacy and where both the sender and all intended recipients are located within the United States; or

(C) the installation or use of an electronic, mechanical, or other surveillance device in the United States to acquire information other than from a wire communication or radio communication under circumstances in which a person has a constitutionally protected right of privacy.

(7) "Attorney General" means the Attorney General of the United States or in his absence the Acting Attorney General.

(8) Minimization procedures means procedures to minimize the acquisition of information that is not foreign intelligence information, to assume that information which is not foreign intelligence information not be maintained, and to assure that information obtained not be used except as provided in section 2526.

§ 2522. Authorization for electronic surveillance for foreign intelligence purposes

Application for a court order under this chapter are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to Federal judges having jurisdiction under section 2523 of this chapter, and a judge to whom an application is made may grant an order, in conformity with section 2525 of this chapter, approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information.

§ 2523. Designation of judges authorized to grant orders for electronic surveillance

(a) The Chief Justice of the United States shall publicly designate seven district court judges, each of whom shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this chapter, except that no judge designated under this subsection shall have jurisdiction of an application for electronic surveillance under this chapter which has been denied previously by another judge designated under this subsection. If any judge designated under this subsection denies an application for an order authorizing electronic surveillance under this chapter, such judge shall provide immediately for the record a complete written statement of the reasons for his decision and, on motion of the United States, direct that the record be transmitted, under seal, to the special court of review established in subsection (b).

(b) The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the presiding judge, from the

United States district courts or courts of appeals who together shall comprise a special court of review which shall have jurisdiction to review the denial of any application made under this chapter. If such special court determines that the application was properly denied, the special court shall immediately provide for the record a complete written statement of the reasons for its decision and, on motion of the United States, direct that the record be transmitted to the Supreme Court, which shall have jurisdiction to review such decision.

(c) All proceedings under this chapter shall be conducted as expeditiously as possible. The record of proceedings under this chapter, including applications made and orders granted, shall be sealed by the presiding judge and shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General.

§ 2524. Application for an order

(a) Each application for an order approving electronic surveillance under this chapter shall be made by a federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 2523 of this chapter. Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this chapter. It shall include the following information:

(1) the identity of the federal officer making the application;

(2) the authority conferred on the applicant by the President of the United States and the approval of the Attorney General to make the application;

(3) the identity or a characterization of the person who is the target of the electronic surveillance;

(4) a statement of the facts and circumstances relied upon by the applicant to justify his belief that—

(i) the target of the electronic surveillance is a foreign power or an agent of a foreign power and

(ii) the facilities or the place at which the electronic surveillance is directed are being used, or are about to be used, by a foreign power or an agent of a foreign power;

(5) a statement of the procedure to minimize the retention, and dissemination and to require expunging of information relating to permanent resident aliens or citizens of the United States that does not relate to the ability of the United States:

(A) to protect itself against actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) to provide for the national defense or the security of the Nation;

(C) to provide for the conduct of the foreign affairs of the United States;

(D) to protect against the terrorist activities of a foreign power or an agent of a foreign power;

(E) to protect itself against the sabotage activities of a foreign power or an agent of a foreign power;

(F) to protect itself against the clandestine intelligence activities of an intelligence service or network of a foreign power, or an agent of a foreign power except, that appropriate

steps shall be taken to insure that information retained which relates solely to the conduct of foreign affairs shall not be maintained in such a manner as to permit the retrieval of such information by reference to a citizen of the United States who is a party to a communication intercepted as provided in this chapter;

(6) a description of the type of information sought and a certification by the Assistant to the President for National Security Affairs or an executive branch official designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President by and with the advice and consent of the Senate that the information sought is foreign intelligence information, that the purpose of the surveillance is to obtain foreign intelligence information and that such information cannot feasibly be obtained by normal investigative techniques; if the target of the electronic surveillance is a foreign power which qualifies as such solely on the basis that it is an entity controlled and directed by a foreign government or governments, and unless there is probable cause to believe that a substantial number of the officers or executives of such entity are officers or employees of a foreign government, or agent of a foreign power as defined in section 2521(2) (B), (C), (D), or (E), a statement of the procedures to prevent the acquisition, retention, and dissemination and to require the expunging of communications of permanent resident aliens and citizens of the United States who are not officers or executives of such entity responsible for those areas of its activities which involve foreign intelligence information.

(7) a factual description of the nature of the information sought;

(8) a certification or certification by the Assistant to the President for National Security Affairs or an executive branch official or official designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President by and with the advice and consent of the Senate—

(A) that the information sought is foreign intelligence information;

(B) that the purpose of the surveillance is to obtain foreign intelligence information;

(C) that such information cannot feasibly be obtained by normal investigative techniques;

(D) including a designation of the type of foreign intelligence information being sought according to the categories described in section 2521 (b) (3); and

(E) including a statement of the basis for the certification that—

(i) the information sought is the type of foreign intelligence information designated, and

(ii) such information cannot feasibly be obtained by normal investigative techniques;

(9) a statement of the period of time for which the electronic surveillance is required to be maintained. If the nature of the in-

telligence gathering is such that the approval of the use of electronic surveillance under this chapter should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter.

(b) The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

(c) At the time of the hearing on the application, the applicant may furnish to the judge additional information and the judge may require the applicant to furnish such other information or evidence as may be necessary to make the determinations required by section 2525 of this chapter.

§ 2525. Issuance of an order

(a) Upon an application made pursuant to section 2524 of this title, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that—

(1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;

(2) the applicaton has been made by a federal officer and approved by the Attorney General;

(3) on the basis of the facts submitted by the applicant there is probable cause to believe that:

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and

(B) the facilities or place at which the electronic surveillance is directed are being used, or are about to be used, by a foreign power or an agent of a foreign power;

(4) minimization procedures to be followed are reasonably designed to minimize the acquisition, retention, and dissemination of, and to require the expunging of information relating to permanent resident aliens or citizens of the United States is not foreign intelligence information, that does not relate to the ability of the United States.

(A) to protect itself against actual or potential attack or other grave hostile acts of a foreign power or agent of a foreign power;

(B) to provide for the national defense or the security of the Nation;

(C) to provide for the conduct of the foreign affairs of the United States;

(D) to protect against the terrorist activities of a foreign power or an agent of a foreign power;

(E) to protect itself against the sabotage activities of a foreign power or an agent of a foreign power;

(F) to protect itself against the clandestine intelligence activities of an intelligence service or network of a foreign power or an agent of a foreign power;

except, that appropriate steps shall be taken to insure that information retained which relates solely to the conduct of foreign affairs shall not be maintained in such a manner as to permit the retrieval of such information by reference to a citizen of the

United States who is a party to a communication intercepted as provided in this chapter.

(5) if the target of the electronic surveillance is a foreign power which qualifies as such solely on the basis that it is an entity controlled and directed by a foreign government or governments, and unless there is probable cause to believe that a substantial number of the officers or executives of such entity are officers or employees of a foreign government, or agents of a foreign power as defined in section 2521(2) (B), (C), (D), or (E), procedures to be followed are reasonably designed to prevent the acquisition, retention, and dissemination and to require the expunging of communications of permanent resident aliens and citizens of the United States who are not officers or executives of such entity responsible for those areas of its activities which involve foreign intelligence information.

(6) the application which has been filed contains the description and certification or certifications specified in section 2524(a) (7) and (8).

(7) certification has been made pursuant to section 2524(a) (6) that the information sought is foreign intelligence information, that the purpose of this surveillance is to obtain such foreign intelligence information and that such information cannot feasibly be obtained by normal investigative techniques.

(b) An order approving an electronic surveillance under this section shall—

(1) specify—

(i) the identity or a characterization of the person who is the subject of the electronic surveillance;

(ii) the nature and location of the facilities or the place at which the electronic surveillance will be directed;

(iii) the type of information sought to be acquired;

(iv) the means by which the electronic surveillance will be effected; and

(v) the period of time during which the electronic surveillance is approved; and

(2) direct—

(i) that the minimization procedures be followed;

(ii) that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, contractor, or other specified person furnish the applicant forthwith any and all information, facilities, or technical assistance, or other aid necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, contractor, or other person is providing that target of electronic surveillance; and

(iii) that the applicant compensate, at the prevailing rates, such carrier, landlord, custodian, or other person for furnishing such aid.

(c) An order issued under this section may approve an electronic surveillance for the period necessary to achieve its purpose, or for ninety days, whichever is less. Extensions of an order issued under this chapter may be granted upon an application for an extension made

in the same manner as required for an original application and after findings required by subsection (a) of this section. In connection with the new findings of probable cause, the judge may require the applicant to submit information obtained pursuant to the original order or to any previous extensions, or any other information or evidence as he finds necessary to such new findings. Each extension may be for the period necessary to achieve the purposes for which it is granted, or for ninety days, whichever is less.

(d) Notwithstanding any other provision of this chapter when the Attorney General reasonably determines that—

(1) an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained, and

(2) the factual basis for issuance of an order under this chapter to approve such surveillance exists,

he may authorize the emergency employment of electronic surveillance if a judge designated pursuant to section 2523 of this title is informed by the Attorney General or his designate at the time of such authorization that the decision has been made to employ emergency electronic surveillance and if an application in accordance with this chapter is made to that judge as soon as practicable, but not more than twenty-four hours after the Attorney General authorizes such acquisition. If the Attorney General authorizes such emergency employment of electronic surveillance, he shall require that the minimization procedures required by this chapter for the issuance of a judicial order be followed. In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of twenty-four hours from the time of authorization by the Attorney General, whichever is earliest. In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated without an order having been issued, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee or other authority of the United States, a State, or a political subdivision thereof. As provided in section 2523, a denial of the application may be appealed by the Attorney General.

(e) A judge denying an order under this section or a panel affirming such denial under section 2523(b) shall state the reasons therefor.

§ 2526. *Use of information*

(a) Information acquired from an electronic surveillance conducted pursuant to this chapter may be used and disclosed by Federal officers and employees only for purposes relating to the ability of the United States—

(1) to protect itself against actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(2) to provide for the national defense or the security of the Nation;

(3) to provide for the conduct of the foreign affairs of the United States;

(4) to protect against the terrorist activities of a foreign power or an agent of a foreign power;

(5) to protect itself against the sabotage activities of a foreign power or an agent of a foreign power;

(6) to protect itself against the clandestine intelligence activities of an intelligence service or network of a foreign power or an agent of a foreign power; or for the enforcement of the criminal law. No otherwise privileged communication obtained in accordance with or in violation of the provisions of this chapter shall lose its privileged character."

(b) The minimization procedures required under this chapter shall not preclude the retention and disclosure, for law enforcement purposes, of any information which constitutes evidence of a crime if such disclosure is accompanied by a statement that such evidence, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(c) No information obtained or derived from an electronic surveillance shall be received in evidence or otherwise used or disclosed in any trial, hearing, or other proceeding in a Federal or State court unless, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to disclose the information or submit it in evidence in the trial, hearing, or other proceeding, the Government notifies the court of the source of the information and the court in camera and ex parte, determines that the surveillance was authorized and conducted in a manner that did not violate any right afforded by the Constitution and statutes of the United States to the person against whom the evidence is to be introduced. In making such a determination, the court, after reviewing a copy of the court order and accompanying application in camera, shall order disclosed to the person against whom the evidence is to be introduced the order and application, or portions thereof, only if it finds that such disclosure would substantially promote a more accurate determination of the legality of the surveillance and that such disclosure would promote a more accurate determination of such legality, that such disclosure would not harm the national security, there is a reasonable question as to the legality of the surveillance or that such disclosure would not harm the national security.

(d) Any person who has been a subject of electronic surveillance and against whom evidence derived from such electronic surveillance is to be, or has been, introduced or otherwise used or disclosed 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 communication acquired by electronic surveillance, 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; or

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

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 communication acquired by electronic surveillance or evidence derived therefrom shall be suppressed. The judge, upon the filing of such motion may in his discretion make available to the person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice and the national security. The judge upon the filing of such motion may, in his discretion make available to the person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(e) If an emergency employment of the electronic surveillance is authorized under section 2525(d) and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States citizen or permanent resident alien named in the application and on such other United States citizen or permanent resident alien subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of—

(1) the fact of the application;

(2) the period of the surveillance; and

(3) the fact that during the period foreign intelligence information was or was not obtained.

On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

§ 2527. *Report of electronic surveillance*

(a) In April of each year, the Attorney General shall report to the Administrative Office of the United States Courts and shall transmit to the Congress with respect to the preceding calendar year—

(1) the number of applications made for orders and extensions of orders approving electronic surveillance and the number of such orders and extensions granted, modified, and denied;

(2) the periods of time for which applications granted authorized electronic surveillances and the actual duration of such electronic surveillances;

(3) the number of such surveillances in place at any time during the preceding year; and

(4) the number of such surveillances terminated during the preceding year.

(b) Nothing in this chapter shall be deemed to limit the authority of the Select Committee on Intelligence of the United States Senate to obtain such information as it may need to carry out its duties pursuant to Senate Resolution 400, 94th Congress, agreed to May 19, 1976.

§ 2528. *Presidential power*

Nothing contained in chapter 119, section 605 of the Communications Act of 1934, or this chapter shall be deemed to affect the exercise of any constitutional power the President may have, subject to determination by the courts, to acquire foreign intelligence information by means of an electronic, mechanical, or other surveillance device if:

(a) such acquisition does not come within the definition of electronic surveillance in paragraph (6) of subsection (b) of section 2521 of this chapter, or

(b) the facts and circumstances giving rise to the acquisition are so unprecedented and potentially harmful to the Nation that they cannot be reasonably said to have been within the contemplation of Congress in enacting this chapter or chapter 119; Provided, That in such an event, the President shall, within seventy-two hours of the initiation of such surveillance, transmit to the Select Committee on Intelligence of the United States Senate and the Committees on the Judiciary of the Senate and House of Representatives, under a written injunction of secrecy if necessary, a statement setting forth the nature of such facts and circumstances.

Foreign intelligence information acquired by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial, hearing, or other proceeding only where such acquisition was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.

Sec. 3. The provisions of this Act and the amendment made hereby shall become effective upon enactment: Provided, That, any electronic surveillance approved by the Attorney General to gather foreign intelligence information shall not be deemed unlawful for failure to follow the procedures of chapter 120, title 18, United States Code, if that surveillance is terminated or an order approving that surveillance is obtained under this chapter within sixty days following the designation of the first judge pursuant to section 2523 of chapter 120, title 18, United States Code.

Sec. 5. On or before March 1, 1978, and on the first day of March of each year thereafter, the Select Committee on Intelligence of the United States Senate shall report to the Senate concerning the implementation of this chapter. Said reports shall include but not be limited to an analysis and recommendations concerning whether this chapter should be (1) amended, (2) repealed, or (3) permitted to continue in effect without amendment.

Sec. 6. (a) In the event the Select Committee on Intelligence of the United States Senate shall report that this chapter should be amended or repealed, it shall report out legislation embodying its recommendations within thirty calendar days, unless the Senate shall otherwise determine by yeas and nays.

(b) Any legislation so reported shall become the pending business of the Senate with time for debate equally divided between the proponents and the opponents and shall be voted on within three calendar days thereafter, unless the Senate shall otherwise determine by yeas and nays.

(c) Such legislation passed by the Senate shall be referred to the appropriate committee of the other House and shall be reported out by such committee together with its recommendations within thirty calendar days and shall thereupon become the pending business of such House and shall be voted upon within three calendar days, unless such House shall otherwise determine by yeas and nays.

(d) In the case of any disagreement between the two Houses of Congress with respect to such legislation passed by both Houses, conferees shall be promptly appointed and the committee of conference

shall make and file a report with respect to such legislation within seven calendar days after the legislation is referred to the committee of conference. Notwithstanding any rule in either House concerning the printing of conference reports in the record or concerning any delay in the consideration of such reports, such report shall be acted on by both Houses not later than seven calendar days after the conference report is filed. In the event the conferees are unable to agree within three calendar days they shall report back to their respective Houses in disagreement.

ADDITIONAL VIEWS OF SENATOR ADLAI STEVENSON

This bill attempts to strike a fair balance between conflicting requirements of national and personal security. In my judgment it comes close to the mark. But the judicial safeguards against executive abuse are fragile. And the safeguards of Congressional review and oversight are virtually nil.

One of the purposes of Subsection (b) of Section 2527, added by the Committee to the Judiciary Committee's bill, was to make clear that the annual report of the Attorney General on electronic surveillance is not adequate fulfillment of the Attorney General's obligation to keep the Committee informed. But the bill does nothing to assure that the Committee is informed on a timely basis of all electronic surveillance cases and in sufficient detail to enable the Committee to exercise its oversight duties under Senate Resolution 400. Consequently, I voted to report the bill but reserved the right to offer an Amendment which would mandate continuous and contemporaneous disclosure to the Committee of information about all surveillance conducted pursuant to this Act.

The Attorney General has cooperated fully with the Committee, and if arrangements can be worked out which assure the Committee continued receipt of adequate information about surveillance and on a timely basis, I will not offer this Amendment. The modalities of a reporting arrangement are being developed by the Committee and the Department of Justice. It is my hope and expectation that the Committee will receive adequate assurances without resort to enactment of a statutory requirement. If not, this bill would be much improved by a statutory assurance that the right of individuals will be safeguarded by Congressional oversight.

ADDITIONAL VIEWS OF SENATOR JOSEPH BIDEN

I am not enthusiastic about S. 3197, even as amended by the Senate Select Committee. However, inasmuch as the Justice Department agreed to a good faith effort to compromise, I am voting to report this bill. The Committee adopted, with a few modifications, an amendment I proposed on the controversial definition of "agent of a foreign power."

My concerns about this bill fall into three major areas: (1) I am still concerned about the constitutionality of this bill; (2) I wish the Committee had modified or eliminated the so-called "inherent authority" provision of the bill; and finally (3) I am concerned that the Committee's action in approving this bill not prejudice its efforts to develop legislative charters for intelligence agencies.

I. THE CONSTITUTIONALITY OF S. 3197

In 1967, in two landmark decisions, *Berger* v. *New York*, 388 U.S. 41, and *Katz* v. *United States*, 389 U.S. 347, the Supreme Court held that the Fourth Amendment to the Constitution applied to electronic surveillance. In essence, that meant that the basic right to privacy of American citizens encompassed private conversations and could not be violated by the government without a compelling need.

The scheme the founding fathers developed, in the Fourth Amendment, to police invasions of privacy has two basic parts. First, an American's privacy cannot be invaded unless a judicial officer issues a warrant authorizing the search and second, the judge must have probable cause to believe that the search will seize particular evidence of specific criminal activity.

Ever since the *Katz* and *Berger* cases the Justice Department has been attempting to engraft exceptions to these standards for national security electronic surveillance. After a brief, and I must say, quite cursory review of the national security electronic surveillance program of the FBI, I now understand why they feel compelled to engraft such an exception upon these rules. Much of their electronic surveillance has not met these two standards. Of course, their inability to meet these standards resulted in dangerous invasion of privacy, including the abusive electronic surveillance revealed by the Church Committee.

This bill is an attempt to regularize national security electronic surveillance through a statutory warrant procedure. Unfortunately the emphasis in drafting this procedure has been upon the first part of the Fourth Amendment, that is the warrant procedure, and not the second, that there be probable cause that the search will seize particular evidence of specific crimes. Therefore, S. 3197, as introduced, had an elaborate warrant procedure for judicial review of requests for electronic surveillance but prohibited the judge from requiring that the

government show that the surveillance would overhear conversations about specific criminal acts threatening to the national security.

To my mind both parts of the Fourth Amendment are of equal importance. After all it was the abuse of so-called "General warrants" and "Writs of assistance" in colonial America and 18th century England which led to the Fourth Amendment. Both of these abusive warrant procedures were used by the British Crown to suppress dissent through the harassment of gross invasions of privacy in the name of enforcing the tax laws in the colonies and the so-called seditious libel laws in Great Britain. The Framers of the Fourth Amendment recognized as the major abuse in these warrant procedures their failure to "particularly describe" the place to be searched or things to be seized. Ironically, these abusive searches, which gave rise to the Fourth Amendment, were also conducted in the name of national security—the revolutionary refusal of our forefathers to be taxed without representation and the propensity of critics of the Crown in 18th century England to engage in seditious libel.

At the beginning of our negotiations, Attorney General Levi insisted that it was impossible for the FBI to comply with both parts of the Fourth Amendment. Indeed, he argued that the FBI did not have to comply with both parts, relying on a series of so-called administrative search Supreme Court cases which permitted looser Fourth Amendment standards. These cases, involving one-time searches of houses violating housing codes or car searches for illegal aliens, simply cannot be relied upon for 90 days of electronic surveillance of Americans who, under the bill as originally proposed, may be engaged in legal political activities (such as lobbying Congress for more arms for Israel or Egypt at the behest of either country).

Apparently, the Attorney General saw the frailty of that argument and in the course of our negotiations, accepted amendments to the definitions section of the bill. These amendments refine such vague terms as "clandestine intelligence activities", so that before authorizing electronic surveillance the judge must be satisfied that the American is engaged in specific acts, with very limited exceptions, criminal acts. It was the Attorney General's movement on this question that convinced me that, in good faith, I should acquiesce with Committee approval of the bill.

I am still troubled by the outcome. We may not have gone far enough to pass constitutional muster. For example, the bill still permits electronic surveillance of some activities which in and of themselves are not criminal. Furthermore, on a more fundamental level this bill goes well beyond existing electronic surveillance law and Fourth Amendment cases and says in effect that where there is probable cause that the subject of a search is engaged in criminal activity there is no need to satisfy the judge that the search will seize evidence of that criminal activity (in the case of electronic surveillance that the subject will engage in criminal conversations on the phone). I have substantial doubts about the constitutionality of that doctrine, although the majority of my colleagues and the Department of Justice do not. As the Supreme Court said in another landmark Fourth Amendment case, the same year it decided *Katz* and *Berger*:

> There must of course be a nexus—automatically provided in the case of fruits, instrumentalities or contraband—

between the item to be seized and criminal behavior. Thus, in the case of "mere evidence", probable cause must be examined in terms of cause to believe that the evidence sought will aid in a particular apprehension or conviction. *Warden* v. *Hayden*, 387 U.S. 294 (1967).

II. THE INHERENT AUTHORITY SECTION

Section 2528 of the bill preserves intact the concept of inherent presidential authority to spy on Americans. This was of course the basic argument in defense of many Watergate illegalities. It is the only authority for the Federal government's huge National Security Agency electronic surveillance program.

The Department of Justice and my colleagues have made an honest effort to write this language with neutrality so that Congress is not on record for or against the doctrine of inherent authority. The reasons for doing so are persuasive. The Federal government must be able to continue its essential NSA Programs directed at hostile foreign powers.

Unfortunately, it may be impossible to write language on this matter which is neutral in effect. Congress is on notice of NSA abuses, including project SHAMROCK and the watchlists both documented by the Church Committee. Congress is on notice of the myriad of abuses engaged in by other intelligence agencies and by non-intelligence officials, in the course of the Watergate matter, undertaken in the name of this doctrine. For Congress to act in this area and deliberately skirt NSA and at the same time leave undisturbed inherent authority may be viewed by some courts as sanctioning the doctrine.

I can imagine defendants in the present FBI burglary investigation arguing that Congress did not abolish the doctrine of inherent authority when it had the chance; that therefore the doctrine exists; and that they were acting pursuant to what they believed was a valid exercise of that doctrine. Indeed any Watergate defendant, and former intelligence official who engaged in illegal surveillance might make that argument.

Furthermore, I am not convinced that Congress is aware of every intelligence program engaged in or planned by the Federal government. What additional programs have been or will be undertaken in the name of "inherent authority" without congressional knowledge? Are we giving a signal to the courts and the Executive branch that there still is an area which we feel is beyond public scrutiny through the Congress in enacting section 2528? That is certainly not the message we intend and I hope that is not the message that is received.

III. THE IMPACT OF S. 3197 ON THE LEGISLATIVE CHARTER DRAFTING

Certainly one of the most troublesome aspects of S. 3197 is its impact upon our efforts to develop meaningful legislation is in effect a "backdoor" charter for foreign intelligence activities.

Unfortunately, we have not had time to have a comprehensive staff or agency briefing on the so-called counterintelligence and positive intelligence activities of the Federal government within the United States. Specifically, we have not carefully examined the existing

statutory authority for such activities. We know, indeed Attorney General Levi has admitted, that there are not adequate statutes for their present programs. This is the reason why we have had to authorize, in the revised definitions of S. 3197, electronic surveillance of Americans not engaged in criminal activities.

We learned in the course of hearings on this bill that the FBI and other components of the federal intelligence community collect information on the clandestine intelligence efforts of foreign nations—counterintelligence. The Federal government is also engaged in so-called positive intelligence programs. As I understand it, positive intelligence includes collection within the United States of information on all the activities of a foreign power or its agents regardless of whether the activities are intended to harm the United States.

In the past the Executive branch has taken a rather expansive view of its responsibilities to seek positive intelligence and counterintelligence. For example, counterintelligence might include not only efforts to counter Soviet espionage programs directed at our military and defense secrets but the relationship of American oil companies to ARAMCO in anticipation of an oil boycott. Positive intelligence could involve not only surveillance to determine the Soviet Union's problem with its wheat harvest, but efforts on the part of Soviet or Indian trade attachés to discreetly contact grain cooperatives in this country in anticipation of seeking grain to supplement their inadequate harvests.

The legal authority for such investigations by the Department of Justice, especially investigations directed at American citizens, is dubious at best. The statute which is usually cited as authority for FBI investigations reads as follows:

> *28 U.S.C. 533. Investigative and other officials; Appointment*
>
> The Attorney General may appoint officials—
>
> (1) to detect and prosecute crimes against the United States;
>
> (2) to assist in the protection of the person of the President; and
>
> (3) to conduct such other investigations regarding official matters under the control of the Department of Justice and the Department of State as may be directed by the Attorney General.
>
> This section does not limit the authority of departments and agencies to investigate crimes against the United States when investigative jurisdiction has been assigned by law to such departments and agencies.

Since such investigations are by definition non-criminal and, of course, unrelated to the protection of the President, all such authority rests on the cryptic "such other investigations" language of 533(3). This vague section has an interesting history. It was originally enacted in the code before the enactment of the Espionage Act of 1917 to provide authority for classic counterespionage investigations. However, the vague language was also the authority which J. Edgar Hoover cited for the initiation of domestic intelligence programs of recent infamy.

The statutes upon which other intelligence agencies base their counterintelligence and positive intelligence responsibilities within the United States are no more precise. The National Security Act which created the Central Intelligence Agency assumed that all of the existing agencies had such intelligence collection authority within the United States. The extent to which it grants such authority to the CIA is not clear at all. The National Security Agency, which conducts by far the largest amount of foreign intelligence (counterintelligence and positive intelligence) electronic collection, is not even a creature of federal statute and furthermore, is completely exempt from the restrictions of the wiretap bill. Indeed, one of the few federal statutes which might be said to confer any foreign intelligence jurisdiction on the Federal government (the Export Administration Act [50 U.S.C. App. § 2401, *et seq.*], setting some limits upon the export of industrial technology) expires in September of this year. [50 U.S.C. App. § 2413]

Therefore the basic federal statutes outlining the prohibited or regulated activities of American citizens who work with foreign governments and the statutes outlining the responsibilities of the intelligence community to investigate such activities are in a complete shambles. Indeed, present state of these statutes is clearly a threat to civil liberties. The ambiguities and conflicting jurisdictions inherent in these statutes undermine the national security as well. We have reluctantly decided to proceed with legislation authorizing electronic surveillance of activities without first clarifying whether they are covered by existing law.

I believe that it is incumbent upon this Committee and the Congress to commit ourselves to revising these statutes and creating meaningful statutory charters and criminal and regulatory statutes in this area. The Americans who routinely deal with foreign entities and the agencies of the intelligence community must both know what their government expects of them in terms of the national security.

I would have preferred to see the Committee create (within the context of S. 3197) an incentive to correct this chaos in the United States Code, a chaos which may permit innocent Americans to unknowingly jeopardize the national security and may lead the intelligence agencies to abuse the rights of Americans. I would have preferred to see a provision of the bill requiring that troublesome areas of S. 3197—warrantless surveillance of Americans by NSA and surveillance of noncriminal activities by all agencies—be terminated in two years unless explicitly authorized in new legislative charters. This assumes that both the Executive branch and the Congress concur on the high priority of setting this area of the law in order. I believe that it can be done within two years and if it cannot by the end of that period Congress can grant an extension. Regardless, the national security, the Constitution and the painful lesson of abuses which have grown out of the failure to clarify these laws require such a commitment. Unfortunately the Department of Justice would accept no such amendment.

In conclusion, I view S. 3197, as amended by the Select Committee, as a definite and substantial improvement over the bill as approved by the Judiciary Committee. I am not sure whether it is an adequate improvement over existing law. I therefore reserve the right to vote against the bill when it reaches the floor.

ADDITIONAL VIEWS OF SENATOR ROBERT MORGAN

While I fully understand the significance of what S. 3197 attempts to do and laud the efforts of those who agree with me that governmental electronic surveillance must be conducted pursuant to a judicial warrant procedure, even in the foreign intelligence field, I am unable to support the bill as it is presently written. In addition to opposing the bill for the substantive reasons advanced by Senator Biden in his additional views, with which I fully concur, I am opposed, as a matter of principle, to the authorization of the most intrusive investigative technique of our intelligence agencies being practically the first act of this Committee.

The wisdom of the Church Committee in recommending that there be established a permanent intelligence oversight committee in the Senate is apparent in the improvements S. 3197 has undergone since it was referred to this Committee. I am still not satisfied, however, that ample evidence has been presented to the Committee to enable it to fully understand the position of the Administration and other supporters of the bill and to, without some doubt, evaluate the conflict between security and liberty, which the Committee will always face, in this instance.

The Committee is charged with the duty of developing legislative charters which will govern the activities of our intelligence agencies. During this process, the Committee will become well versed in the actual needs of our intelligence community and may decide it is in the best interest of our Nation to substantially alter our present system of laws. At that time, I may be able to support legislation which would legitimize intelligence activities to the possible deprivation of rights of American citizens. Until that time, until the compelling need for change is affirmatively demonstrated, I cannot support a substantial alteration of our existing laws, which I believe this bill to be.

ROBERT MORGAN.